

09/6473/8 日 本 国 特 許 庁

17.02.00 #8

JP 00/904

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 03 MAR 2000

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。This is to certify that the annexed is a true copy of the following application as filed
with this Office.出願年月日
Date of Application:

1999年 2月 17日

Eku

出願番号
Application Number:

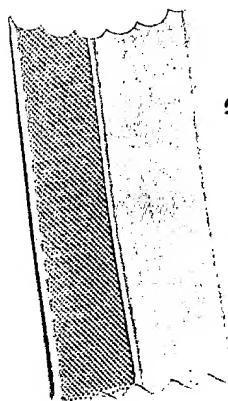
平成11年特許願第039218号

出願人
Applicant(s):

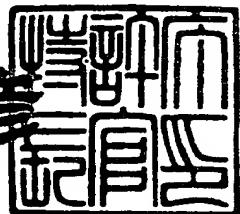
ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

1999年12月17日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特平11-3088138

【書類名】 特許願
【整理番号】 9900113903
【提出日】 平成11年 2月17日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 19/00
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内
【氏名】 河上 達
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内
【氏名】 石黒 隆二
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内
【氏名】 田辺 充
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内
【氏名】 江面 裕一
【特許出願人】
【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代表者】 出井 伸之
【代理人】
【識別番号】 100082131
【弁理士】
【氏名又は名称】 稲本 義雄

【書類名】 明細書

【発明の名称】 情報処理装置および方法、並びに提供媒体

【特許請求の範囲】

【請求項1】 データを蓄積する蓄積手段と、

前記蓄積手段に対するデータの蓄積または読み出しを制御するソフトウェアからなる制御手段と、

前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段と

を含み、

前記制御手段は、前記実行手段の実行結果に基づいて、前記蓄積手段に対するデータの蓄積または読み出しを制御する

ことを特徴とする情報処理装置。

【請求項2】 前記蓄積手段は、蓄積しているデータを管理する管理情報を蓄積しており、

前記制御手段は、前記実行手段に、前記管理情報に基づいて所定の演算を実行させる

ことを特徴とする請求項1に記載の情報処理装置。

【請求項3】 前記制御手段は、CPUであり、

前記蓄積手段は、ハードディスクであり、

前記実行手段は、前記制御手段としてのCPUとは別の半導体ICに組み込まれたCPUである

ことを特徴とする請求項1に記載の情報処理装置。

【請求項4】 データを蓄積する蓄積手段と、

前記蓄積手段に対するデータの蓄積または読み出しを制御するソフトウェアからなる制御手段と、

前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段と

を含む情報処理装置の情報処理方法において、
前記制御手段は、前記実行手段の実行結果に基づいて、前記蓄積手段に対する
データの蓄積または読み出しを制御する制御ステップを含む
ことを特徴とする情報処理方法。

【請求項5】 データを蓄積する蓄積手段と、
前記蓄積手段に対するデータの蓄積または読み出しを制御するソフトウェアか
らなる制御手段と、
前記制御手段から供給された、暗号化されているプログラムを復号して実行し
、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェ
アに設けられた実行手段と
を含む情報処理装置の前記制御手段に、
前記実行手段の実行結果に基づいて、前記蓄積手段に対するデータの蓄積また
は読み出しを制御する制御ステップ
を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供する
ことを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、改竄を防
止し、不正な複製を抑制することができるようとした、情報処理装置および方法
、並びに提供媒体に関する。

【0002】

【従来の技術】

最近、デジタル技術の普及にともない、音楽データ、画像データなどの各種の
データがデジタル的に記録媒体に記録または再生されるようになってきた。その
結果、複数回コピーしても、画質あるいは音質が劣化しないデータを得ることが
可能となってきた。

【0003】

【発明が解決しようとする課題】

しかしながら、このようにデジタル技術が発達してくると、次のような問題が発生する。

【0004】

(1) 例えば、コンパクトディスク (CD) からパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、CDからの音楽データが、そのまま、あるいは圧縮符号化されてハードディスクに記録されるので、例えば、インターネットなどのネットワークを介して複製を違法に大量に配布することができてしまう。

【0005】

(2) CDからパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、そのコピーの回数に制限がないため、複製が大量に配布されてしまう。

【0006】

(3) パーソナルコンピュータのハードディスク内のデジタル音楽データを、例えば、メモリスティックウォークマン（商標）などの外部の機器に移す場合、移した後もハードディスク内に元のデジタル音楽データが残るので、複製が大量に配布できてしまう恐れがある。

【0007】

(4) 上記した(3)の問題を防止するために、デジタル音楽データを外部の機器に移した後に、データの送り元としてのハードディスクのデータを消去するように（いわゆる、音楽データをムーブするように）パーソナルコンピュータのソフトウェアを作成しておけばよいが、例えば、ムーブの前にハードディスクの内容を別の記録媒体へバックアップしておき、ムーブの後に、バックアップしたデータをハードディスクにリストアすれば、結局、ムーブしたはずのデータがハードディスクに残ってしまうことになる。

【0008】

(5) パーソナルコンピュータが、ハードディスク内のデジタル音楽データ

をメモリスティックウォークマンなどの外部の機器に移す場合、外部機器がどのような機器であるかを確認しないため、違法な機器にデジタル音楽データが渡されてしまう恐れがある。

【0009】

(6) メモリスティックウォークマンなどの外部の機器から、パーソナルコンピュータにデジタル音楽データを渡す場合、そのパーソナルコンピュータを制御しているソフトウェアがどのようなソフトウェアであるかを確認しないため、違法なソフトウェアに対してデジタル音楽データが渡されてしまう恐れがある。

【0010】

(7) CDより再生された音楽データをパーソナルコンピュータで取り扱うとき、複数の曲が同一か否かを判断するために、曲データに含まれるISRC (International Standard Recording Code) を使用することが可能であるが、CDによっては、ISRCデータを含んでいないものがある。この場合、複数の曲が同一であるか否かを判定することができなくなる。

【0011】

(8) 以上のような各機能は、パーソナルコンピュータ上で、ソフトウェアの制御により実現されるため、そのソフトウェアが改竄されると、システムの作成者が意図しない動作を行わせることができてしまう。

【0012】

本発明はこのような状況に鑑みてなされたものであり、ソフトウェアを解析し、改竄することで、不正な複製が大量に生成されてしまうようなことを確実に防止することができるようとするものである。

【0013】

【課題を解決するための手段】

請求項1に記載の情報処理装置は、データを蓄積する蓄積手段と、蓄積手段に対するデータの蓄積または読み出しを制御するソフトウェアからなる制御手段と、制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を制御手段に供給する、制御手段とは独立したハードウェアに設けられた実行手段とを含み、制御手段は、実行手段の実行結果に基づいて、蓄積手段に

に対するデータの蓄積または読み出しを制御することを特徴とする。

【0014】

請求項4に記載の情報処理方法は、制御手段は、実行手段の実行結果に基づいて、蓄積手段に対するデータの蓄積または読み出しを制御する制御ステップを含むことを特徴とする。

【0015】

請求項5に記載の提供媒体は、実行手段の実行結果に基づいて、蓄積手段に対するデータの蓄積または読み出しを制御する制御ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0016】

請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載の提供媒体においては、ソフトウェアからなる制御手段は、ハードウェアに設けられた実行手段の実行結果に基づいて、蓄積手段に対するデータの蓄積または読み出しを制御する。

【0017】

【発明の実施の形態】

図1は、本発明を適用したネットワークシステムの構成例を表している。パーソナルコンピュータ1は、各種の処理を実行するCPU(Central Processing Unit)12、各種のプログラムやデータを一時的に記憶するメモリ13、並びに、各種のプログラムやデータを大量に蓄積するハードディスク15を備えている。CD-ROM(Read Only Memory)ドライブ14は、装着されたCD-ROMに記録されているプログラムやデータを読み出す。IEC(International Electrotechnical Commission)60958端子16aを有する音声入出力インターフェース16は、デジタル音声入出力、あるいはアナログ音声入出力のインターフェース処理を実行する。インターネット接続インターフェース11は、インターネット4との間のインターフェース処理を実行する。インターフェース17は、アダプタ3またはメモリスティックウォークマン2との間のインターフェース処理、並びに、入力部2およびディスプレイ3に対するインターフェース処理を実行する。

【0018】

半導体ICとして、一体的に形成され、パーソナルコンピュータ1に装着されるアダプタ3のCPU32は、インターフェース31を介してパーソナルコンピュータ1のCPU12と共に働し、各種の処理を実行する。RAM33は、CPU32が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ34は、パーソナルコンピュータ1の電源がオフされた後も保持する必要があるデータを記憶する。ROM36には、パーソナルコンピュータ1から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC(Real Time Clock)35は、計時動作を実行し、時刻情報を提供する。

【0019】

メモリスティックウォーム2は、不揮発性メモリ23を有し、パーソナルコンピュータ1からインターフェース21と認証装置22を介して提供されたデジタル音楽データを記憶する。認証装置22は、パーソナルコンピュータ1と不揮発性メモリ23との間でデータを授受するとき、相互に認証処理を実行する。インターフェース21は、パーソナルコンピュータ1との間のインターフェース処理、あるいは不揮発性メモリ23に記憶されている音楽データを読み出し、ヘッドホンなどを介してユーザに提供するためのインターフェース処理を実行する。

【0020】

パーソナルコンピュータ1は、インターネット4を介してEMD(Electrical Music Distribution)サーバ5と接続されており、EMDサーバ5から音楽データの提供を受けることができる。

【0021】

次に、図2のフローチャートを参照して、CD-ROMドライブ14に装着されたCDから再生した音楽データをハードディスク15に転送し、コピーする場合の処理について説明する。ユーザが入力部2を操作して、インターフェース17を介してCPU12に対してCD-ROMドライブ14に装着されたCD(図示せず)から再生された音楽データをハードディスク15に転送、コピーする指令を入力すると、CPU12は、ステップS11において、インターフェース17を介してディスプレイ3

にコピーする曲を選択するためのGUI (Graphical User Interface) を表示させる。

【0022】

具体的には、例えば、CPU12は、CD-ROMドライブ14に装着されたCDのTOC (Table Of Contents) を読み込み、そのCDに含まれる曲の情報を得て、ディスプレイ3に表示させる。または、CPU12は、CDに含まれている各曲毎のISRC (International Standard Recording Code) を読み出し、その曲の情報を得て、ディスプレイ3に表示させる。あるいはまた、CPU12は、インターネット4を介して外部のデータベースにアクセスし、TOCを用いて、そのCDの曲の情報を得て、対応するGUIをディスプレイ3に表示させる。ユーザは、ディスプレイ3のGUIを利用して入力部2を操作し、コピーする曲を選択する。

【0023】

次に、ステップS12において、CPU12は、ハードディスク15に記憶されている期限データベースをチェックする。この期限データベースチェック処理の詳細は、図3のフローチャートに示されている。

【0024】

ステップS31においてCPU12は、アダプタ7のCPU32と共に働いて、期限データベース全体のハッシュ値を計算し、ステップS32において、その計算された値と、前回保存しておいたハッシュ値と比較する。

【0025】

すなわち、ハードディスク15には、期限データベースが形成されており、この期限データベースには、図4に示すように、ハードディスク15に記録されている音楽データを管理する管理情報として、過去に記録されたことのある曲のISRC番号とコピー日時が対応して記憶されている。この例においては、アイテム1乃至アイテム3の3つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全ての曲のISRC番号とコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップS38において、アダプタ7のCPU32により計算され、不揮発性メモリ34に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得

られた値である。ハッシュ関数は、一般的に可変長の長いデータを、固定長の短い値にマップする一方向性の関数であり、ハッシュ値同士の衝突が起こりにくい性質を有している。ハッシュ関数の例としては、SHA、MD5などがある。CPU12は、ステップS31において、CPU32が実行したのと同様にハッシュ値を計算する。そして、ステップS32において、CPU12は、CPU32に、不揮発性メモリ34に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップS31で、いま自分自身が計算したハッシュ値とを比較する。

【0026】

ステップS33において、CPU12は、ステップS31でいま計算したハッシュ値と、不揮発性メモリ34に記憶されている前回の期限データベースのハッシュ値とが一致するか否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、CPU12は、ステップS34において、例えば、「期限データベースが改竄されたので、コピーができません」といったメッセージを発生し、インターフェース17を介してディスプレイ3に出力し、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されている音楽データを再生し、ハードディスク15にコピーする処理が禁止される。

【0027】

ステップS31で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップS35に進み、CPU12は、ステップS11で指定されたコピーする曲として選択された曲（選択曲）のISRC番号をCDから取得する。CDにISRC番号が記録されていない場合、CPU12は、そのCDのTOCのデータを読み出し、そのデータにハッシュ関数を適用するなどして、例えば、58ビットなどの適当な長さのデータを得て、これをISRC番号に代えて用いる。

【0028】

ステップS36において、CPU12は、ステップS35で取得したISRC番号（すなわち、選択曲）が期限データベース（図4）に登録されているか否かを判定する。ISRC番号が期限データベースに登録されていない場合には、その曲はまだハードディスク15に記録されていないことになるので、ステップS37に進み、CPU12は、その曲のISRC番号と現在の日時とを期限データベースに登録する

。なお、CPU1 2は、この現在の日時として、CPU3 2から転送を受けた、アダプタ7のRTC3 5が出力する値を利用する。そして、ステップS3 8において、CPU1 2は、その時点における期限データベースのデータを読み出し、アダプタ7のCPU3 2に転送する。CPU3 2は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ3 4に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップS3 2において、前回保存しておいたハッシュ値として利用される。

【0029】

次に、ステップS3 9において、CPU1 2は、選択曲が期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図2のステップS1 3において、選択曲が期限データベースに登録されているか否かの判定を行うときに用いられる。

【0030】

ステップS3 6において、選択曲のISRC番号が期限データベースに登録されていると判定された場合、その選択曲は、少なくとも一度、ハードディスク1 5に登録されたことがある曲であるということになる。そこで、この場合、ステップS4 0に進み、CPU1 2は、期限データベースに登録されているその選択曲の登録日時より、現在の日時（アダプタ7のRTC3 5が出力した現在の日時）が4 8時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に4 8時間以上経過している場合には、ハードディスク1 5に、少なくとも一度は記録したことがあるが、既に、その時から4 8時間以上経過しているので、その曲を再度コピーさせたとしても、それほど実害がないので、この場合には、ハードディスク1 5へのコピーが許容される。そこで、ステップS4 1に進み、CPU1 2は、期限データベースの日時を、過去の登録日時から現在の日時（RTC3 5の出力する日時）に変更させる。そして、ステップS3 8に戻り、CPU1 2は、再び、期限データベース全体のハッシュ値をCPU3 2に計算させ、不揮発性メモリ3 4に保存させるとともに、ステップS3 9において、その曲に対して未登録のフラグを設定する。

【0031】

一方、ステップS40において、現在時刻が登録日時より、まだ48時間以上経過していないと判定された場合、その選択曲のハードディスク15へのコピーが禁止される。そこで、この場合には、ステップS42に進み、CPU12は、その選択曲に対応して登録済みのフラグを設定する。

【0032】

以上のようにして、期限データベースチェック処理により、選択曲がハードディスク15に登録されているか否かを表すフラグが設定される。

【0033】

図2に戻り、ステップS13においてCPU12は、選択曲が期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択曲が登録済みである場合には、ステップS14に進み、CPU12は、ディスプレイ3に、例えば、「この曲は一度コピーされてからまだ48時間以上経過していないので、コピーすることができません」のようなメッセージを表示させる。これにより、ユーザーは、その曲をハードディスク15にコピーすることができない理由を知ることができる。

【0034】

ステップS13において、選択した曲が期限データベースに登録されていないと判定された場合、ステップS15に進み、CPU12は、CD-ROMドライブ14を制御し、そこに装着されているCDから音楽データを読み出させる。この音楽データには、図5に示すように、所定の位置にウォータマークコードが挿入されている。CPU12は、ステップS16において、音楽データに含まれているウォータマークコードを抽出し、そのウォータマークコードがコピー禁止を表しているか否かをステップS17において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップS18に進み、CPU12は、インターフェース17を介してディスプレイ3に、例えば、「コピーは禁止されています」のようなメッセージを表示させ、コピー処理を終了させる。

【0035】

これに対して、ステップS17において、ウォータマークがコピー禁止を表し

ていないと判定された場合、ステップS19に進み、CPU12は、音楽データを、例えば、ATRAC (Adaptive Transform Acoustic Coding) (商標) などの方式で、ソフトウェア処理により圧縮させる。ステップS20において、CPU12は、予め設定され、メモリ13に記憶されている暗号鍵を用いて、例えば、DES (Data Encryption Standard) 方式、FEAL (Fast Encipherment Algorithm) 方式などの暗号化方法により、音楽データを暗号化する。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ7のCPU32により発生させた乱数に基づいて生成したもの用いることもできる。このように、パソコン用コンピュータ1だけではなく、それに付随して装着されたハードウェアとしてのアダプタ7のCPU32と、共働して暗号化処理を実行するようにすることでき、解読がより困難となる暗号化を行うことが可能となる。

【0036】

次に、ステップS21において、CPU12は、暗号化されたデータをハードディスク15に転送し、1つのファイルとしてファイル名を付けて保存させる。あるいはまた、1つのファイルの一部として、そのファイル名の位置情報（例えば、先頭からのバイト数）を与えて保存するようにしてもよい。

【0037】

この保存処理と、上記した圧縮符号化処理および暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

【0038】

さらに、ステップS22において、CPU12は、予め定められているメモリ13に記憶されている保存用鍵を使って、上述したDES方式、FEAL方式などの方式で、音楽データを暗号化した暗号鍵を暗号化し、ハードディスク15の曲データベースに保存する。

【0039】

ステップS23において、CPU12は、保存したファイルに関する情報、暗号化された暗号鍵、その曲の情報、ユーザがGUIを介して入力した曲名の情報の要素を組にしてハードディスク15の曲データベースに登録する。そして、ステップS24において、CPU12は、CPU32に、曲データベース全体のハッシュ値を

計算させ、不揮発性メモリ34に保存させる。

【0040】

このようにして、例えば、図6に示すような曲データベースが、ハードディスク15上に登録される。この例においては、アイテム1乃至アイテム3のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ、およびコピー条件（SCMS）が記録されている。

【0041】

次に、図7乃至図9のフローチャートを参照して、ハードディスク15からメモリスティックウォークマン6の不揮発性メモリ23（メモリスティック）に、音楽データを移動する処理について説明する。ステップS51において、CPU12は、曲データベース全体のハッシュ値を計算し、ステップS52で、前回CPU32に計算させ、不揮発性メモリ34に保存しておいたハッシュ値と比較する。両者が一致しない場合、CPU12は、ステップS53に進み、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ3に表示させた後、処理を終了させる。この場合の処理は、図3のステップS31乃至ステップS34の処理と同様の処理である。この場合においては、ハードディスク15からメモリスティックウォークマン6への音楽データの移動が実行されないことになる。

【0042】

次に、ステップS54において、CPU12は、ハードディスク15に形成されている曲データベースから、そこに登録されている曲の情報を読み出し、ディスプレイ3に、選択のためのGUIとして表示させる。ユーザは、この選択のためのGUIに基づいて、ハードディスク15からメモリスティックウォークマン6へ移動させる曲を、入力部2を操作して選択する。次に、ステップS55において、CPU12は、ステップS54で選択された選択曲の再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図10のフローチャートを参照して後述する。

【0043】

次に、ステップS56において、パーソナルコンピュータ1のCPU12とメモリスティックウォークマン6の認証装置22との間において、相互認証処理が行われ、通信用鍵が共有される。

【0044】

例えば、メモリスティックウォークマン6の不揮発性メモリ23には、マスター鍵 K_M が予め記憶されており、パーソナルコンピュータ1のメモリ13には、個別鍵 K_p とIDが予め記憶されているものとする。認証装置22は、CPU12から、メモリ13に予め記憶されているIDの供給を受け、そのIDと自分自身が有するマスター鍵 K_M にハッシュ関数を適用して、メモリ13に記憶されているパーソナルコンピュータ1の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ1とメモリスティックウォークマン6の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

【0045】

あるいはまた、パーソナルコンピュータ1のメモリ13にIDとマスター鍵 K_{MP} を予め記憶しておくとともに、メモリスティックウォークマン6の不揮発性メモリ23にもメモリスティックウォークマン6のIDとマスター鍵 K_{MM} を記憶させておく。そして、それぞれのIDとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたIDとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようとする。

【0046】

なお、認証の方法としては、例えば、IOS (International Organization for Standardization) 9798-2を利用することができる。

【0047】

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップS57において、CPU12は、選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データ（例えば、図2のステ

ップS20の処理で暗号化されている)をハードディスク15から読み出す。ステップS58において、CPU12は、ステップS57で読み出したデジタル音楽データの圧縮符号化方式(ステップS19の処理)、暗号化方式(ステップS20の処理)、フォーマットなどをメモリスティックウォークマン6のものに変換する処理を実行する。この変換処理の詳細は、図12のフローチャートを参照して後述する。

【0048】

ステップS59において、CPU12は、ステップS58で変換した音楽データを、ステップS56の相互認証処理により共有した通信用鍵で暗号化し、メモリスティックウォークマン6にインターフェース17を介して転送する。ステップS60において、メモリスティックウォークマン6の認証装置22は、インターフェース21を介してこの伝送されてきた音楽データを受信すると、その音楽データを、そのまま不揮発性メモリ23に記憶させる。

【0049】

ステップS61において、CPU12は、さらに、曲データベースに登録されているその選択曲の再生条件(開始日時、終了日時、回数制限など)を、メモリスティックウォークマン6が管理している形式に変換する。ステップS62において、CPU12は、さらに選択曲の曲データベース中に登録されているコピー条件中のSCMS情報を、メモリスティックウォークマン6の管理する形式に変換する。そして、ステップS63において、CPU12は、ステップS61で変換した再生条件と、ステップS62で変換したSCMS情報を、メモリスティックウォークマン6に転送する。メモリスティックウォークマン6の認証装置22は、転送を受けた再生条件とSCMS情報を、不揮発性メモリ23に保存する。

【0050】

ステップS64において、CPU12はまた、選択曲の曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU12が曲データベース中で扱っている形式のまま、メモリスティックウォークマン6に転送し、不揮発性メモリ23に保存させる。

【0051】

ステップS65において、CPU12は、選択曲の暗号化されている暗号鍵を曲データベースから読み出し、ステップS66において、その暗号鍵をメモリ13に保存されている保存用鍵で復号し、通信用鍵で暗号化する。そして、通信用鍵で暗号化した暗号鍵を、CPU12は、メモリスティックウォークマン6に転送する。

【0052】

メモリスティックウォークマン6の認証装置22は、ステップS67で、パソコン用コンピュータ1から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、不揮発性メモリ23に保存する。

【0053】

認証装置22は、暗号鍵の保存が完了すると、ステップS68において、パソコン用コンピュータ1に対して暗号鍵を保存したことを探知する。パソコン用コンピュータ1のCPU12は、メモリスティックウォークマン6からこの通知を受けると、ステップS69において、ハードディスク15から、その音楽データのファイルを削除するとともに、曲データベースからその曲の要素の組を削除する。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップS70において、CPU12は、アダプタ7のCPU32に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ34に保存させる。このハッシュ値が、上述したステップS52において、前回保存しておいたハッシュ値として用いられることになる。

【0054】

次に、図7のステップS55における選択曲の再生条件などのチェック処理について説明する。ステップS81において、CPU12は、曲データベースから、各種の条件を読み出す。CPU12は、ステップS82において、ステップS81で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップS83に進み、CPU12

は、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ3に表示させ、処理を終了させる。ステップS82において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップS84に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ7のRTC35より出力されたものが用いられる。これにより、ユーザが、パーソナルコンピュータ1の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。CPU12は、この現在日時をCPU32から提供を受けて、ステップS84の判断を自ら行うか、または、ステップS81で、曲データベースから読み出した再生条件をアダプタ7のCPU32に供給し、CPU32に、ステップS84の判定処理を実行させる。

【0055】

現在日時が再生終了日時を過ぎている場合、ステップS85に進み、CPU12は、選択曲をハードディスク15から消去するとともに、曲データベースから、その選択曲の情報を消去する。ステップS86において、CPU12は、CPU32に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ34に保存させる。以後、処理は終了される。従って、この場合、音楽データの移動が実行されない。

【0056】

ステップS84において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップS87に進み、CPU12は、その選択曲の再生時課金条件（例えば、再生1回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、CPU12は、ステップS88において、メモリスティックウォークマン6と通信し、メモリスティックウォークマン6に課金機能が存在するか否かを判定する。メモリスティックウォークマン6に課金機能が存在しない場合には、選択曲をメモリスティックウォークマン6に転送する訳にはいかないので、ステップS89において、CPU12は、例えば、「転送先が課金機能を有しておりません」のようなメッセージをディスプレイ3に表示させ、音楽データの移動処理を終了させる。

【0057】

ステップS87において再生時課金条件が登録されていないと判定された場合、または、ステップS88において、メモリスティックウォークマン6に課金機能が存在すると判定された場合、ステップS90に進み、CPU12は、選択曲に関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップS91に進み、CPU12は、メモリスティックウォークマン6に、その再生条件を守る機能が存在するか否かを判定する。メモリスティックウォークマン6が、その再生条件を守る機能を有していない場合には、ステップS92に進み、CPU12は、例えば、「転送先の装置が再生条件を守る機能を有しておりません」のようなメッセージをディスプレイ3に表示させ、処理を終了させる。

【0058】

ステップS90において、再生条件が登録されていないと判定された場合、またはステップS91において、メモリスティックウォークマン6が再生条件を守る機能を有している判定された場合、再生条件等のチェック処理が終了され、図7のステップS56に戻る。

【0059】

図11は、メモリスティックウォークマン6が管理している（守ることが可能な）再生条件の例を表している。この例においては、アイテム1乃至アイテム3の各曲について、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム2についてのみ登録されており、アイテム1とアイテム3については登録されていない。従って、アイテム2の曲が選択曲とされた場合、再生回数の再生条件は守ることが可能であるが、アイテム1またはアイテム3の曲が選択曲とされた場合、再生回数の条件は守ることができないことになる。

【0060】

次に、図12のフローチャートを参照して、図7のステップS58におけるフォーマット変換処理の詳細について説明する。ステップS101において、CPU12は、ハードディスク15に記録されている選択曲のフォーマット（再生条件、使用条件、コピー条件など）を調べる。ステップS102において、CPU12

は、相手先の機器（今の場合、メモリスティックウォークマン6）に設定することが可能な条件を調べる。すなわち、CPU12は、メモリスティックウォークマン6の認証装置22に設定可能な条件を問い合わせ、その回答を得る。ステップS103においてCPU12は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップS102で調べた条件に基づいて決定する。

【0061】

ステップS104において、CPU12は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップS105に進み、音楽データをメモリスティックウォークマン6に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をメモリスティックウォークマン6が守ることができないので、そのようなメモリスティックウォークマン6には、音楽データを移動することが禁止されるのである。

【0062】

ステップS104において設定可能な条件が存在すると判定された場合、ステップS106に進み、CPU12は、その条件を相手先の機能フォーマットの条件に変換する。そして、ステップS107において、変換した条件を相手先の機器に設定する。その結果、メモリスティックウォークマン6は、設定された条件に従って（その条件を守って）、音楽データ再生することが可能となる。

【0063】

次に、図13乃至図15のフローチャートを参照して、ハードディスク15からメモリスティックウォークマン6に音楽データをコピーする場合の処理について説明する。この図13乃至図15のステップS111乃至ステップS127の処理は、図7乃至図9のハードディスク15からメモリスティックウォークマン6へ音楽データを移動させる場合のステップS51乃至ステップS67の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択曲の再生条件とのチェック処理が行われる。さらに、メモリスティックウォークマン6と、パーソナルコンピュータ1との間の相互認証処理の後、音楽データが、パーソナルコンピュータ1のハードディスク15からメ

モリスティックウォークマン6の不揮発性メモリ23に転送され、保存される。その後、ステップS128において、パーソナルコンピュータ1のCPU12は、曲データベースのコピー回数カウンタを1だけインクリメントする。そして、ステップS129において、CPU12は、CPU32に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ34に保存させる。

【0064】

次に、図16のフローチャートを参照して、メモリスティックウォークマン6からハードディスク15に音楽データを移動する処理について説明する。ステップS161において、パーソナルコンピュータ1のCPU12は、メモリスティックウォークマン6の認証装置22に対して不揮発性メモリ23に記憶されている曲の情報の読み出しを要求する。認証装置22は、この要求に対応して、不揮発性メモリ23に記憶されている曲の情報をパーソナルコンピュータ1に送信する。パーソナルコンピュータ1のCPU12は、この情報に基づいて、ディスプレイ3に、不揮発性メモリ23に記憶されている曲を選択するためのGUIを表示させる。ユーザは、入力部2を操作して、そのGUIに基づいて、メモリスティックウォークマン6からハードディスク15に移動させる曲を指定する。

【0065】

ステップS162において、CPU12は、認証装置22との間において、相互認証処理を実行し、通信用鍵を共有する。この処理は、図7のステップS56における場合と同様の処理である。

【0066】

次に、ステップS163において、認証装置22は、不揮発性メモリ23に記憶されている暗号化されている選択曲の音楽データを読み出し、パーソナルコンピュータ1に転送する。パーソナルコンピュータ1のCPU12は、ステップS164において、メモリスティックウォークマン6から転送されてきた音楽データを、1つのファイルとしてファイル名を付けて、ハードディスク15に保存する。この保存は、例えば、1つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

【0067】

ステップS165において、認証装置22は、不揮発性メモリ23に記憶されている選択曲の暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ1に転送する。この暗号鍵は、例えば、図9のステップS67の処理で不揮発性メモリ23に保存されていたものである。

【0068】

ステップS166において、パーソナルコンピュータ1のCPU12は、メモリステイックウォークマン6から暗号鍵の転送を受けると、それを通信用鍵で復号し、自分自身の保存用鍵で暗号化する。ステップS167で、CPU12は、ステップS164で保存した音楽データのファイルのファイル名、その曲の情報をユーザがGUIを介して入力した曲名、ステップS166で暗号化した暗号鍵などを、ハードディスク15の曲データベースに登録する。そして、ステップS168において、CPU12は、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0069】

ステップS169において、パーソナルコンピュータ1のCPU12は、メモリステイックウォークマン6に対して暗号鍵が保存されたことを通知し、その曲の音楽データの削除を要求する。認証装置22は、パーソナルコンピュータ1から、その曲の音楽データの削除が要求されてきたとき、ステップS170において、不揮発性メモリ23に記憶されているその曲の音楽データを削除する。

【0070】

次に、メモリステイックウォークマン6からハードディスク15へ音楽データをコピーする場合の処理について、図17のフローチャートを参照して説明する。この図17に示すステップS181乃至ステップS188の処理は、図16のメモリステイックウォークマン6からハードディスク15へ音楽データを移動させる場合の処理におけるステップS161乃至ステップS168の処理と同様の処理である。すなわち、コピー処理の場合は、図16のステップS169、S170の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理と

なるので、その説明は省略する。

【0071】

次に、図18のフローチャートを参照して、EMDサーバ5から転送を受けた音楽データをハードディスク15にコピーする処理について説明する。ステップS201において、CPU12は、入力部2を介してユーザからEMDサーバ5へのアクセスが指令されたとき、インターネット接続インターフェース11を制御し、インターネット4を介してEMDサーバ5にアクセスさせる。EMDサーバ5は、このアクセスに対応して、自分自身が保持している曲の曲番号、曲名、各情報などの情報を、インターネット4を介してパーソナルコンピュータ1に転送する。パーソナルコンピュータ1のCPU12は、インターネット接続インターフェース11を介して、この情報を取得したとき、それをインターフェース17を介してディスプレイ3に表示させる。ユーザは、ディスプレイ3に表示されたGUIを利用して、ステップS202において、コピーを希望する曲を指定する。この指定情報は、インターネット4を介してEMDサーバ5に転送される。ステップS203において、CPU12は、EMDサーバ5との間において、インターネット4を介して相互認証処理を実行し、通信用鍵を共有する。

【0072】

パーソナルコンピュータ1とEMDサーバ5との間で行われる相互認証処理は、例えば、ISO 9798-3で規定される公開鍵と秘密鍵を用いて行うようになることができる。この場合、パーソナルコンピュータ1は、自分自身の機密鍵とEMDサーバ5の公開鍵を予め有しており、EMDサーバ5は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ1の公開鍵は、EMDサーバ5から転送したり、あるいはパーソナルコンピュータ1に予め配布されているcertificateをパーソナルコンピュータ1からEMDサーバ5に転送し、そのcertificateをEMDサーバ5が確認し、公開鍵を得るようにしてよい。さらに、ステップS204において、CPU12は、EMDサーバ5との間において課金に関する処理を実行する。この課金の処理の詳細は、図19のフローチャートを参照して後述する。

【0073】

次に、ステップS205において、EMDサーバ5は、パーソナルコンピュータ1に対して、ステップS202で指定された曲の暗号化されている音楽データをインターネット4を介してパーソナルコンピュータ1に転送する。このとき、時刻情報も適宜転送される。ステップS206において、CPU12は、転送を受けた音楽データをファイル名を付けてハードディスク15に1つのファイルとして保存する。ステップS207において、EMDサーバ5は、さらに、その曲の暗号鍵をステップS203でパーソナルコンピュータ1と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ1へ転送する。

【0074】

CPU12は、ステップS208において、EMDサーバ5より転送を受けた暗号鍵を単独で、またはアダプタ7のCPU32と共同して通信用鍵を用いて復号し、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化する。ステップS209において、CPU12は、その曲のファイル名、曲の情報、ユーザが入力した曲名、暗号化された暗号鍵を組にして、ハードディスク15の曲データベースに登録する。さらに、ステップS210において、CPU12は、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0075】

なお、ステップS205においてEMDサーバ5は、音楽データとともに、時刻データをパーソナルコンピュータ1に送信する。この時刻データは、パーソナルコンピュータ1からアダプタ7に転送される。アダプタ7のCPU32は、パーソナルコンピュータ1より転送されてきた時刻データを受信すると、ステップS211において、RTC35の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ7のRTC35の時刻情報を修正するようにしたので、アダプタ7を常に正しい時刻情報を保持することが可能となる。

【0076】

次に、図19のフローチャートを参照して、図18のステップS204における課金に関する処理の詳細について説明する。ステップS221において、パー

ソナルコンピュータ1のCPU12は、ステップS201でEMDサーバ5から伝送されてきた価格情報の中から、ステップS202で指定された選択曲の価格情報を読み取り、これをハードディスク15上の課金ログに書き込む。図20は、このような課金ログの例を表している。この例においては、ユーザは、アイテム1乃至アイテム3を、EMDサーバ5からコピーしており、アイテム1とアイテム2の領域は50円とされ、アイテム3の料金は60円とされている。その時点における課金ログのハッシュ値も、CPU32により計算され、不揮発性メモリ34に登録されている。

【0077】

次に、ステップS222において、パーソナルコンピュータ1のCPU12は、ステップS221で書き込んだ課金ログをハードディスク15から読み出し、これをインターネット4を介してEMDサーバ5に転送する。EMDサーバ5は、ステップS223において、パーソナルコンピュータ1から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMDサーバ5は、内蔵するデータベースに、パーソナルコンピュータ1のユーザから伝送されてきた課金ログを追加更新する。そして、ステップS224において、EMDサーバ5は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップS225に進み、EMDサーバ5は、決裁に必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップS226において、決裁サーバは、パーソナルコンピュータ1のユーザに対する決裁処理を実行する。ステップS224において、決裁は直ちには行われないと判定された場合、ステップS225とS226の処理はスキップされる。すなわち、この処理は、例えば、月に1回など、定期的にその後実行される。

【0078】

次に、図21と図22のフローチャートを参照して、音声入出力インタフェース16のIEC60958端子16aから入力された、図示せぬCDプレーヤなどからの再生音楽データを、ハードディスク15にコピーする場合の処理について説明する。ステップS241において、ユーザは、CDプレーヤのIEC60958出力端子を、パーソナルコンピュータ1の音声入出力インタフェース16のIEC6

0958端子16aに接続する。ステップS242において、ユーザは、入力部2を操作し、CDプレーヤからコピーする曲の曲名を入力する。そして、ステップS243においてユーザは、CDプレーヤのボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ1との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ1の入力部2を介して再生開始指令を入力することで、CDプレーヤにCDの再生を開始させることも可能である。

【0079】

CDプレーヤにおいて、CDの再生が開始されると、ステップS244において、CDプレーヤから出力された音楽データが、IEC60958端子16aを介してパーソナルコンピュータ1に転送されてくる。ステップS245において、CPU12は、IEC60958端子16aを介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。このSCMSデータには、コピー禁止、コピー1回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップS246において、CPU12は、SCMSデータがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップS247に進み、CPU12は、ディスプレイ3に、例えば、「コピーが禁止されています」といったメッセージを表示させ、コピー処理を終了する。すなわち、この場合には、ハードディスク15へのコピーが禁止される。

【0080】

CPU12は、ステップS246において、ステップS245で読み取ったSCMS情報がコピー禁止を表していないと判定した場合、ステップS248に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップS249において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップS247に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

【0081】

ステップS249において、ウォータマークがコピー禁止を表していないと判定された場合、ステップS250に進み、期限データベースチェック処理が行わ

れる。期限データベースチェックの結果、選択曲が既に登録されていれば、ステップS251, S252の処理で、処理が終了される。この処理は、図2のステップS13, S14の処理と同様の処理である。

【0082】

選択曲がまだハードディスク15に登録されていない曲であれば、ステップS253乃至S258で、その登録処理が実行される。このステップS253乃至ステップS258の処理は、ステップS257において、IEC60958端子から供給されてくるSCMS情報も曲データベースに登録される点を除き、図2のステップS19乃至ステップS24の処理と同様の処理であるので、その説明は省略する。

【0083】

次に、図23と図24のフローチャートを参照して、音楽データをハードディスク15からIEC60958端子16aに出力（再生）する場合の処理について説明する。ステップS271乃至ステップS273において、図13のステップS111乃至S113における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップS274に進み、CPU12は、ハードディスク15の曲データベースにアクセスし、そこに登録されている曲の情報を読み出し、ディスプレイ3に表示させる。ユーザは、その表示を見て、入力部2を適宜操作して、再生出力する曲を選択する。ステップS275において、CPU12は、選択曲の再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図25のフローチャートを参照して後述する。

【0084】

次に、ステップS276において、CPU12は、ステップS274において選択された曲の暗号鍵を曲データベースから読み出し、保存用鍵で復号する。ステップS277において、CPU12は、選択曲のSCMS情報を曲データベースから読み出し、IEC60958端子から出力するSCMS情報を、SCMSシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は1だけイ

ンクリメントされ、新たなSCMS情報とされる。ステップS278において、CPU12はさらに、選択曲のISRCを曲データベースから読み出す。

【0085】

次に、ステップS279において、CPU12は、曲データベースから選択曲ファイル名を読み出し、そのファイル名を基に、その音楽データをハードディスク15から読み出す。CPU12はさらに、その音楽データに対応する暗号鍵を曲データベースから読み出し、保存用鍵で復号し、復号した暗号鍵を用いて、暗号化されている音楽データを復号する。CPU12は、さらに、その音楽データの圧縮符号を復号する。ステップS280において、CPU12は、ステップS279で、復号したデジタル音楽データを、ステップS277で決定したSCMS情報、並びにステップS278で読み出したISRC情報とともに、IEC60958の規定に従って、IEC90958端子16aから出力する。さらにまた、デジタル音楽データをアナログ化し、音声入出力インターフェース16のアナログ出力端子から出力する。

【0086】

ステップS281において、CPU12は、曲データベース中の再生回数カウタの値を1だけインクリメントする。そして、ステップS282において、選択曲に再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS283に進み、CPU12は、対応する料金を課金ログに書き込み、ステップS284において、曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に記憶させる。ステップS282において、選択曲に再生時課金条件が付加されていないと判定された場合、ステップS283とステップS284の処理はスキップされる。

【0087】

次に、図25のフローチャートを参照して、図23のステップS275の再生条件等のチェック処理の詳細について説明する。ステップS301において、CPU12は、曲データベースの各種条件を読み出す。ステップS302においてCPU12は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップS303に進み、選択曲をハードディスク1

5から削除させるとともに、曲データベースから選択曲の情報を削除させる。ステップS304において、CPU12はさらに、曲データベースの新たなハッシュ値をCPU32に計算させ、そのハッシュ値を不揮発性メモリ34に保存させる。この場合、再生出力は禁止される。

【0088】

ステップS302において、再生回数が制限回数を過ぎていないと判定された場合、ステップS305に進み、CPU12は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した場合と同様にステップS303において、選択曲をハードディスクから削除せるとともに、曲データベースからも削除させる。そして、ステップS304において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

【0089】

ステップS305において、再生終了日時が現在日時を過ぎていないと判定された場合は、ステップS306に進み、CPU32は、その選択曲に対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS307に進み、CPU12は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ3に表示させる。ステップS306において、再生時課金条件が付加されていないと判定された場合、ステップS307の処理はスキップされる。

【0090】

次に、図26と図27のフローチャートを参照して、ハードディスク15からメモリスティックウォークマン6経由で音楽データを出力（再生）する場合の処理について説明する。ステップS321乃至ステップS325において、曲データベースの改竄チェックと選択曲の指定、並びに選択曲の再生条件等のチェック処理が行われる。その処理は、図23のステップS271乃至ステップS275の処理と同様の処理であるので、その説明は省略する。

【0091】

ステップS326において、メモリスティックウォークマン6とパーソナルコ

ンピュータ1の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップS327において、パーソナルコンピュータ1のCPU12は、メモリスティックウォークマン6に対して、これから送る暗号化音声データを再生するように命令する。ステップS328において、CPU12は、ステップS324で指定された選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データをハードディスク15から読み出す。CPU12は、ステップS329において、音楽データの圧縮符号化方式、暗号化方式、フォーマットなどをメモリスティックウォークマン6の方式のものに変換する処理を実行する。そして、ステップS330において、CPU12は、ステップS329において変換した音楽データを通信用鍵で暗号化し、メモリスティックウォークマン6に転送する。

【0092】

ステップS331において、メモリスティックウォークマン6の認証装置22は、ステップS327において、パーソナルコンピュータ1から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップS332において、CPU12は、曲データベースの再生回数カウントを1だけインクリメントする。さらに、ステップS333において、CPU12は、選択曲に再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップS334において、その料金を課金ログに書き込み、ステップS335において、CPU32に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択曲に再生時課金条件が付加されていない場合には、ステップS334、ステップS335の処理はスキップされる。

【0093】

本発明においては、音楽データが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU12を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

【0094】

さらに、上述したように、CPU12の機能の一部は、ハードウェアとしてのア

ダプラ7に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

【0095】

例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプラ7の不揮発性メモリ34に保存される。すなわち、図3のステップS32、S33などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ34に記憶されているものとされる。これにより、例えば、ハードディスク15に保存されている音楽データを、他の記録媒体にコピーまたは移動させる前に、ハードディスク15の記録内容をバックアップしておき、ハードディスク15から、そこに保存されている音楽データを他の記録媒体にコピーまたはムーブした後、ハードディスク15にバックアップしておいたデータを再びリストアするようにして、実質的に再現なく、コピーまたはムーブができてしまうようなことが防止される。

【0096】

例えば、図28に示すように、ハードディスク15に曲A、Bが保存されている場合、不揮発性メモリ34には、曲Aと曲Bの情報に対応するハッシュ値が保存されている。この状態において、ハードディスク15の記録データを他の記録媒体51にバックアップしたとする。その後、ハードディスク15に保存されている曲Aと曲Bのうち、曲Aを他の記録媒体52に移動させた場合、その時点において、ハードディスク15に記録されている曲は、曲Bだけとなるので、不揮発性メモリ34のハッシュ値も、曲Bに対応するハッシュ値に変更される。

【0097】

従って、その後、記録媒体51にバックアップしておいたハードディスク15の内容をハードディスク15にリストアして、ハードディスク15に、再び曲Aと曲Bを保存させたとしても、不揮発性メモリ34には、曲Bの情報から演算されたハッシュ値が記憶されており、曲Aと曲Bの情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、ハードディスク15に記憶されている曲Aと曲Bに基づくハッシュ値が、不揮発性メモリ34に記憶され

ている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、ハードディスク15に保存されている曲Aと曲Bの利用が制限されてしまうことになる。

【0098】

さらに、上述したように、アダプタ7は、RTC35を内蔵しており、このRTC35の値は、正しい認証結果が得られた他の装置（例えば、EMDサーバ5）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ1が管理するものではなく、RTC35が出力するものが利用される。従って、ユーザが、パーソナルコンピュータ1の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れようなことができなくなる。

【0099】

また、アダプタ7は、暗号化されて転送されてきたプログラムをROM36に予め記憶しているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図29のフローチャートを参照して説明する。

【0100】

すなわち、パーソナルコンピュータ1は、アダプタ7に対して、所定の処理を実行させたいとき、ステップS351において、アダプタ7に実行させるべきプログラムをメモリ13に予め記憶している暗号鍵を用いて暗号化してアダプタ7に転送する。アダプタ7のROM36には、パーソナルコンピュータ1から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。CPU32は、このROM36に記憶されているプログラムに従って、パーソナルコンピュータ1から転送されてきた暗号化されているプログラムをステップS352において復号する。そして、ステップS313において、CPU32は、復号したプログラムをRAM33に展開し、ステップS354において、そのプログラムを実行する。

【0101】

例えば、上述したように、パーソナルコンピュータ1のCPU12は、ハードデ

イスク15の曲データベースのハッシュ値をアダプタ7に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ7のCPU32に転送する。CPU32は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ34に記憶させる。あるいは、そのハッシュ値を、CPU32は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ1のCPU12に転送する。

【0102】

図30は、アダプタ7の内部のより具体的な構成を表している。アダプタ7は、半導体ICとして形成される。アダプタ7は、図1に示したインターフェース31、CPU32、RAM33、不揮発性メモリ34、RTC35、ROM36以外に、RAM33に対する書き込みと読み出しを制御するRAMコントローラ61、並びに論理回路62を有している。論理回路62は、例えば、暗号化されている音楽データを解読した後、解読したデータをアダプタ7から直接出力する場合の処理のために用いられる。

【0103】

これらのインターフェース31乃至ROM36、RAMコントローラ61、並びに論理回路62は、半導体IC内に一体的に組み込まれ、外部からは分解できないように構成されている。

【0104】

水晶振動子71は、アダプタ7が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路72は、RTC35を動作させるための発振回路である。バッテリ73は、発振回路72、不揮発性メモリ34、およびRTC35に対してバックアップ用の電力を供給している。アダプタ7のその他の回路には、パーソナルコンピュータ1の電源供給回路81からの電力が供給されている。

【0105】

不揮発性メモリ34は、書き込み消去可能なROMで構成することも可能であるが、バッテリ73からのバックアップ電源でバックアップされるRAMで構成する

場合には、例えば、図31に示すように、不揮発性メモリ34の上に保護アルミニウム層91を形成し、さらに、その保護アルミニウム層91と同一平面上となるように、不揮発性メモリ34にバッテリ73からの電力を供給する電源パターン92を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ34を改竄すべく、保護アルミニウム層91を削除しようとすると、同一平面上の電源パターン92も削除されてしまい、不揮発性メモリ34に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

【0106】

さらに、図32に示すように、不揮発性メモリ34に対するデータの書き込みまたは読み出しのための配線101-1乃至101-3は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線101-3からデータを読み出すためには、上方の配線101-1, 101-2を除去しなければならず、複数の配線101-1, 101-2, 101-3から同時にデータを読み取ることができなくなる。さらにまた、この配線101-1乃至101-3を冗長に形成し、直接プローブすると、その付加容量により、その内容を解析することが困難になるようにすることができる。

【0107】

以上においては、記録媒体として、メモリスティックウォークマン6を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。

【0108】

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

【0109】

以上のように、本発明によれば、次のような効果を奏することができる。

【0110】

(1) ハードディスク15に暗号化してデータを記録するとともに、暗号鍵

も保存用鍵で暗号化した上でハードディスク15に記録するようにしたので、ハードディスク15に記録されている音楽データをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

【0111】

(2) 所定の曲を1回コピーしたとき、一定時間（上記例の場合、48時間）の間、その曲をコピーすることができないようするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

【0112】

さらにデータベースを更新する度に、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

【0113】

(3) 外部の装置に音楽データを渡したら、ハードディスク15上の音楽データを消去するようにしたので、ハードディスク15内に元のデジタル音楽データが残らず、その複製を大量に配布することが防止される。

【0114】

(4) ハードディスク15内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、ハードディスク15の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをハードディスク15にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

【0115】

(5) パーソナルコンピュータ1が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

【0116】

(6) 外部機器から、パーソナルコンピュータ1に対してデータを渡す前に、パーソナルコンピュータ1のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対して音楽データを渡

してしまうようなことが防止される。

【0117】

(7) 曲の同一性の判定にISRCを用い、ISRCが取得できないときは、TOCを用いるようにしたので、ISRCが取得できなくとも、曲の同一性を判定することが可能になる。

【0118】

(8) パーソナルコンピュータ1におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ1に外付けされるアダプタ7に負担させるようにしたので、パーソナルコンピュータ1のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

【0119】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0120】

なお、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0121】

【発明の効果】

以上の如く、請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載の提供媒体によれば、蓄積手段に対するデータの蓄積または読み出しを、ハードウェアに設けられた実行手段の実行結果に基づいて、ソフトウェアからなる制御手段により制御するようにしたので、ソフトウェアを解析し、改竄することで、不正にデータを複製することを確実に防止することが可能となる。

【図面の簡単な説明】

【図1】

本発明を適用したシステムの構成例を示すブロック図である。

【図2】

図1のシステムにおいてコンパクトディスクからハードディスク15にコピーする場合の処理を説明するフローチャートである。

【図3】

図2のステップS12の期限データベースチェック処理を説明するフローチャートである。

【図4】

期限データベースの例を示す図である。

【図5】

ウォータマークを説明する図である。

【図6】

曲データベースの例を示す図である。

【図7】

図1のシステムのハードディスク15からメモリスティックウォークマン6へデータを移動する動作を説明するフローチャートである。

【図8】

図1のシステムのハードディスク15からメモリスティックウォークマン6へデータを移動する動作を説明するフローチャートである。

【図9】

図1のシステムのハードディスク15からメモリスティックウォークマン6へデータを移動する作を説明するフローチャートである。

【図10】

図7のステップS55の選択曲の再生条件などのチェック処理を説明するフローチャートである。

【図11】

メモリスティックウォークマンが管理している再生条件を説明する図である。

【図12】

図7のステップS58のフォーマット変換処理の詳細を説明するフローチャートである。

【図13】

図1のハードディスク15からメモリスティックウォークマン6へデータをコピーする場合の動作を説明するフローチャートである。

【図14】

図1のハードディスク15からメモリスティックウォークマン6へデータをコピーする場合の動作を説明するフローチャートである。

【図15】

図1のハードディスク15からメモリスティックウォークマン6へデータをコピーする場合の動作を説明するフローチャートである。

【図16】

図1のメモリスティックウォークマン6からハードディスク15へデータを移動する場合の動作を説明するフローチャートである。

【図17】

図1のシステムのメモリスティックウォークマン6からハードディスク15へデータをコピーする場合の動作を説明フローチャートである。

【図18】

図1のシステムのEMDサーバ5からハードディスク15へデータをコピーする場合の処理を説明するフローチャートである。

【図19】

図18のステップS204の課金に関する処理の詳細を説明するフローチャートである。

【図20】

課金ログを説明する図である。

【図21】

図1のシステムのIEC60958端子16aからハードディスク15へデータをコピーする2合の処理を説明するフローチャートである。

【図22】

図1のシステムのIEC60958端子16aからハードディスク15へデータをコピーする場合の処理を説明するフローチャートである。

【図23】

図1のシステムのハードディスク15からIEC60958端子16aにデータを出力する場合の動作を説明するフローチャートである。

【図24】

図1のシステムのハードディスク15からIEC60958端子16aにデータを出力する場合の動作を説明するフローチャートである。

【図25】

図23のステップS275の再生条件などのチェック処理を説明するフローチャートである。

【図26】

図1のシステムのハードディスク15からメモリスティックウォークマン6経由でデータを出力する場合の動作を説明するフローチャートである。

【図27】

図1のシステムのハードディスク15からメモリスティックウォークマン6経由でデータを出力する場合の動作を説明するフローチャートである。

【図28】

図1の不揮発性メモリ34の機能を説明する図である。

【図29】

図1のシステムのアダプタ7の動作を説明するフローチャートである。

【図30】

図1のシステムのアダプタ7の内部の構成を示す図である。

【図31】

図31の不揮発性メモリ34の内部の構成例を示す図である。

【図32】

図31の不揮発性メモリ34の内部の構成例を示す図である。

【符号の説明】

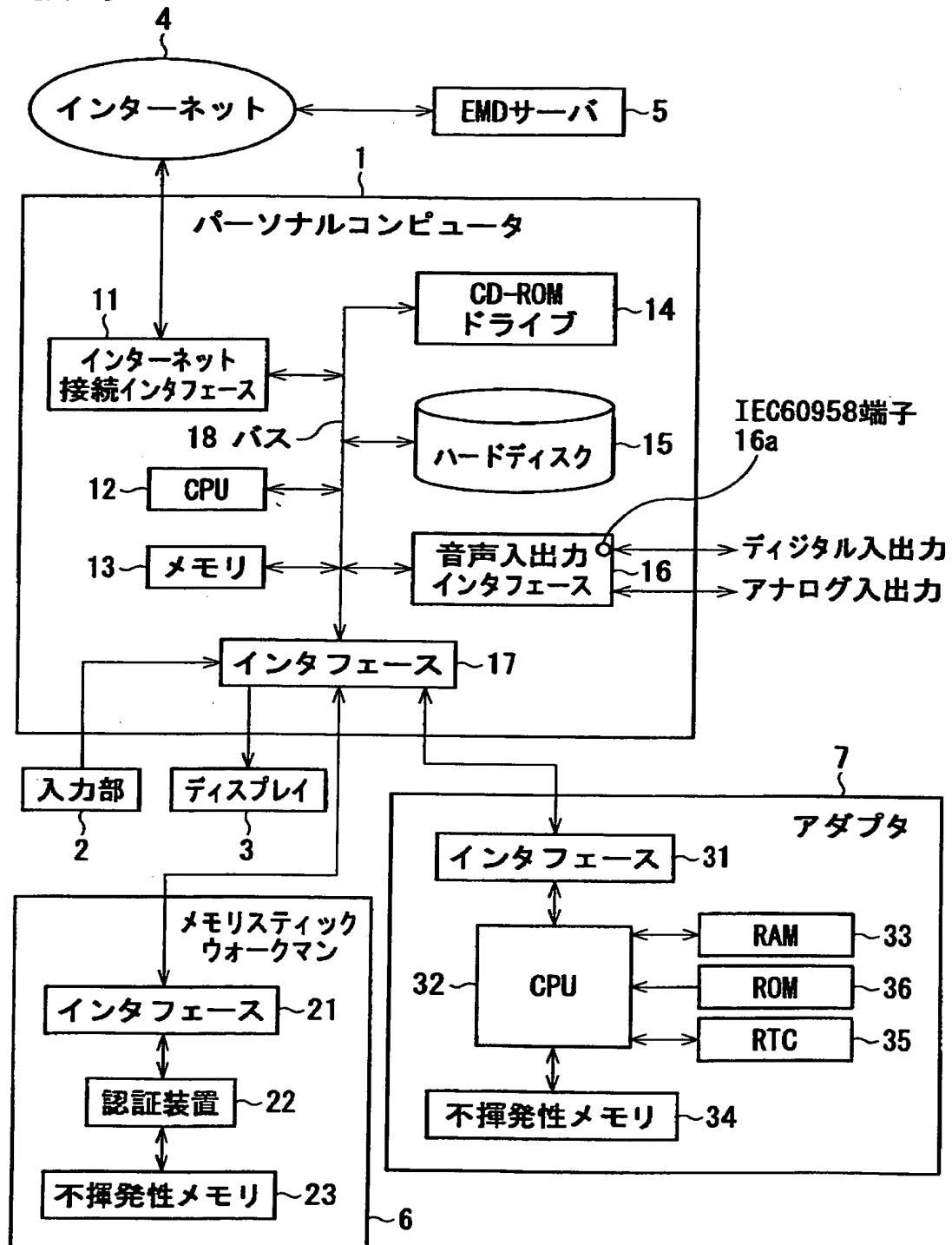
1 パーソナルコンピュータ, 2 入力部, 3 ディスプレイ, 4 インターネット, 5 EMDサーバ, 6 メモリスティックウォークマン, 7 アダプタ, 12 CPU, 13 メモリ, 14 CD-ROMドライブ, 15

特平11-039218

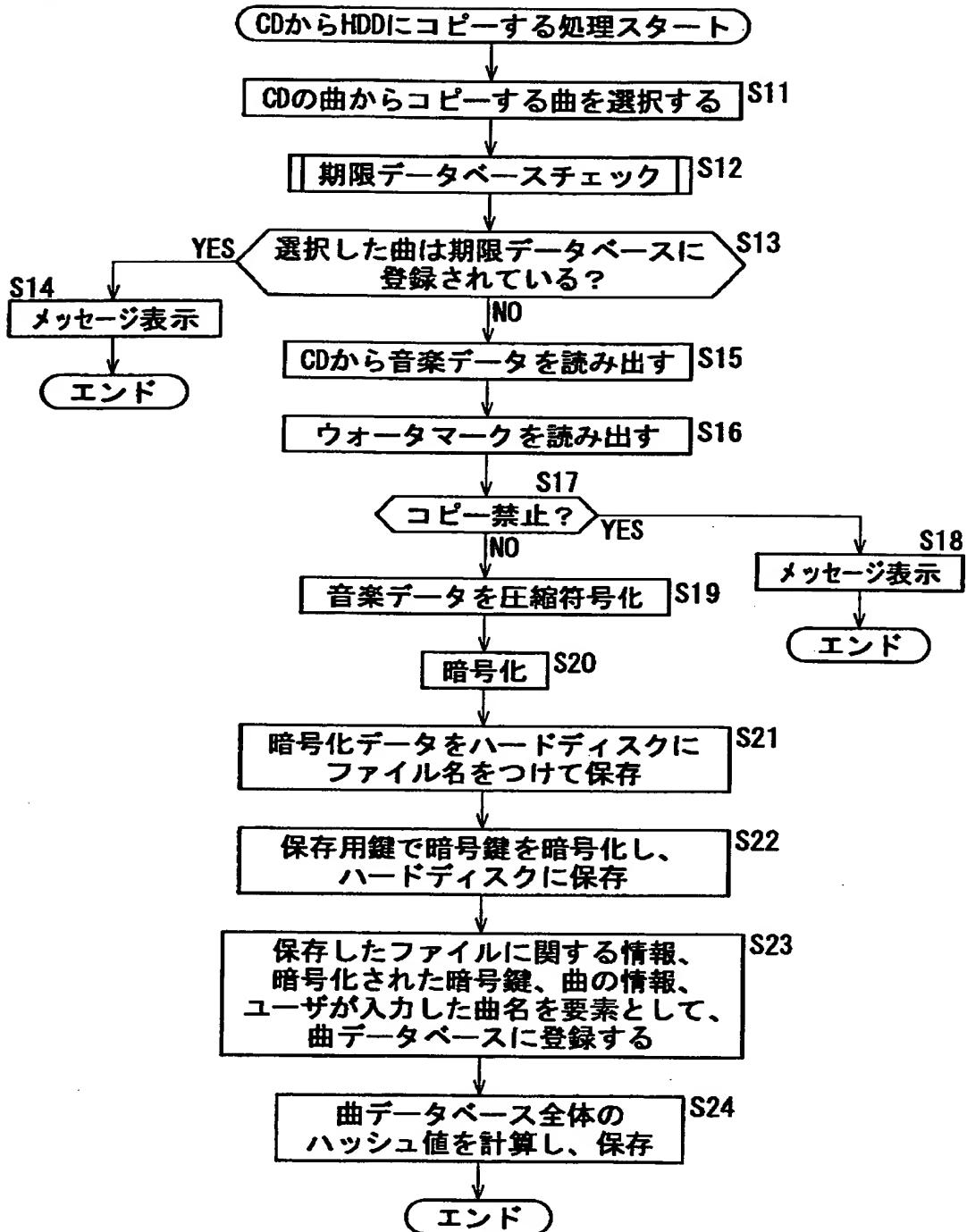
ハードディスク, 16 音声入出力インターフェース, 16a IEC609
58端子, 22 認証装置, 23 不揮発性メモリ, 32 CPU

【書類名】図面

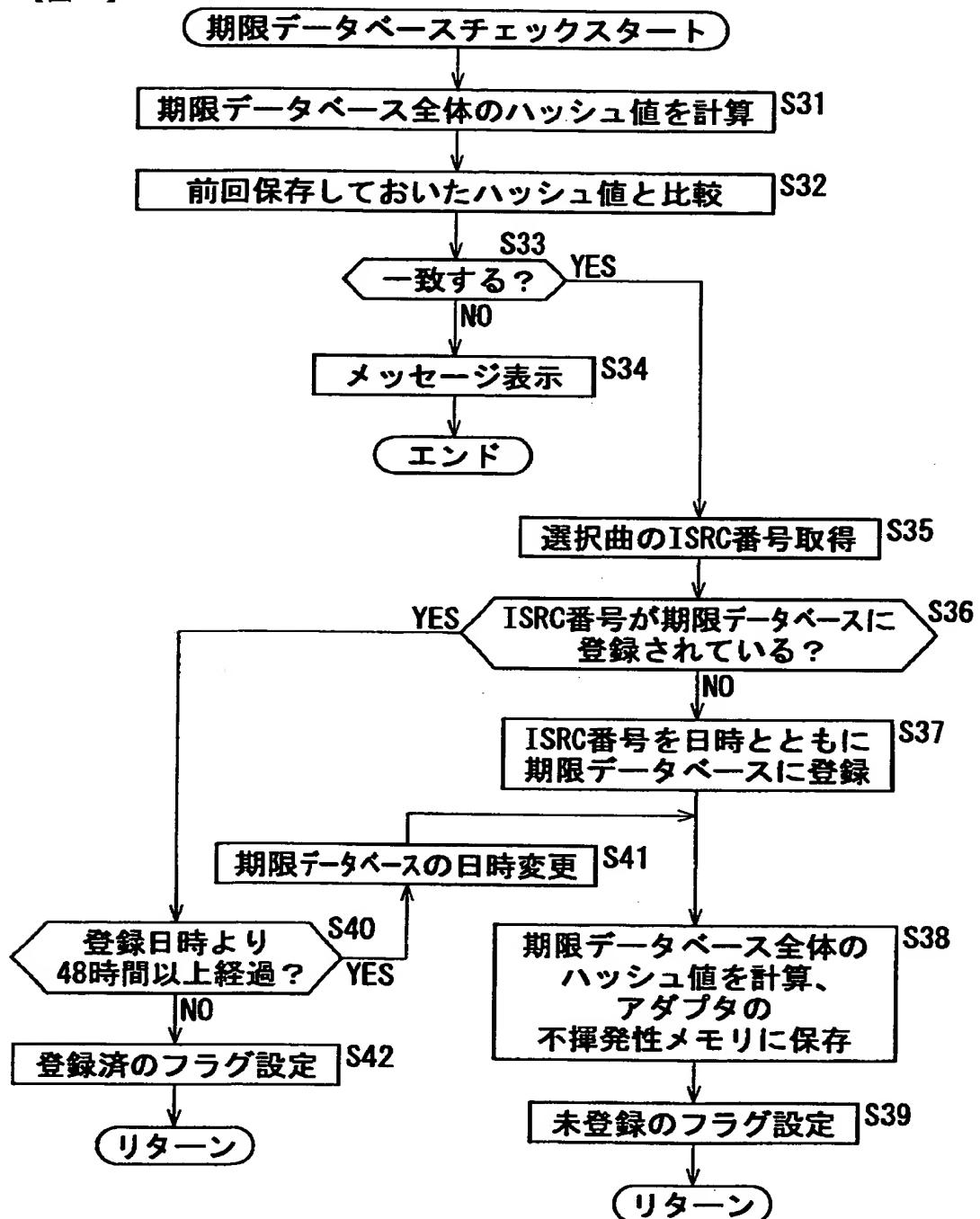
【図1】



【図2】



【図3】



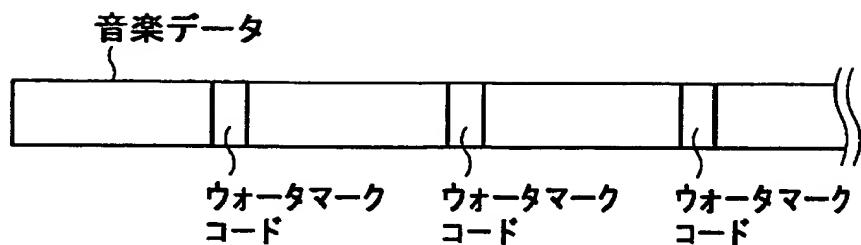
【図4】

期限データベース

	アイテム1	アイテム2	アイテム3
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15

ハッシュ値 0xf3352e125934

【図5】



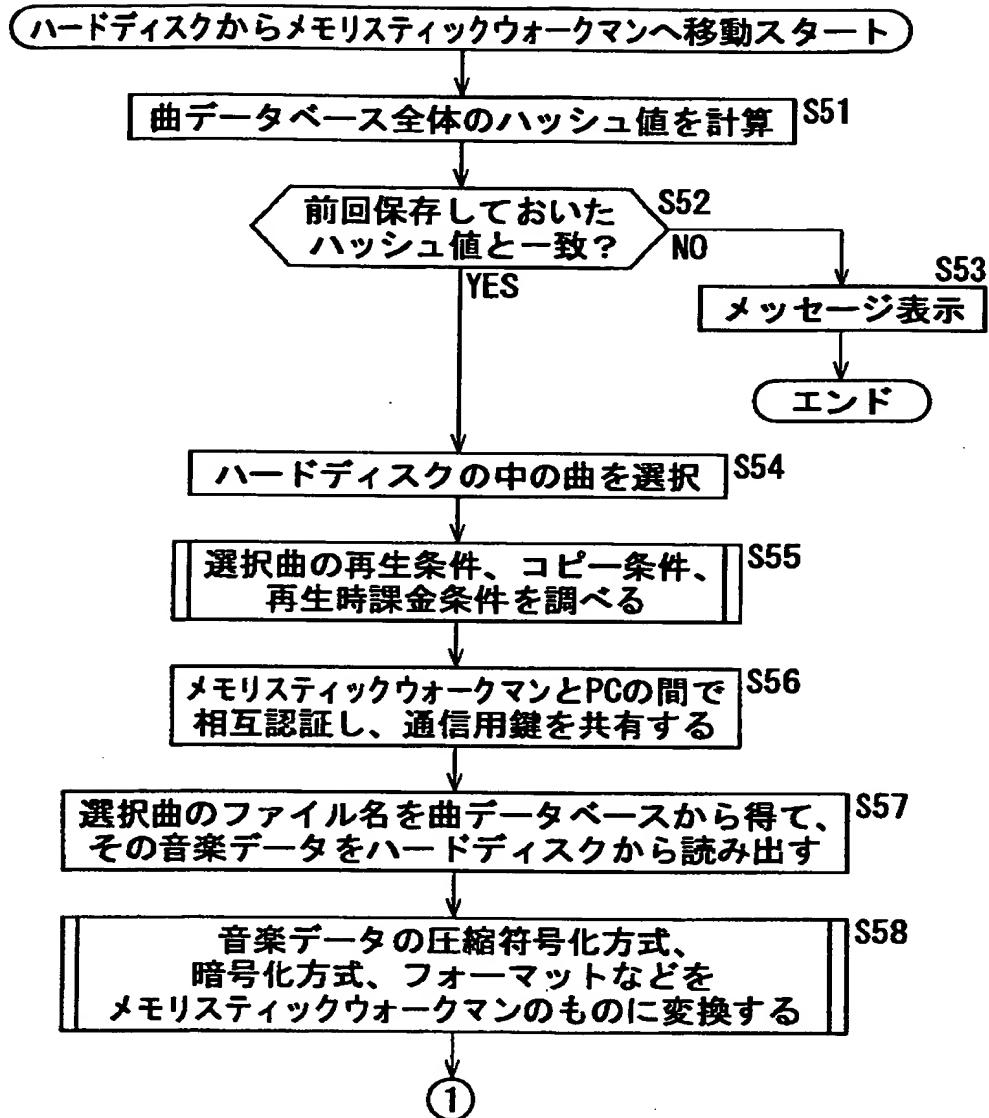
[図6]

曲データベース

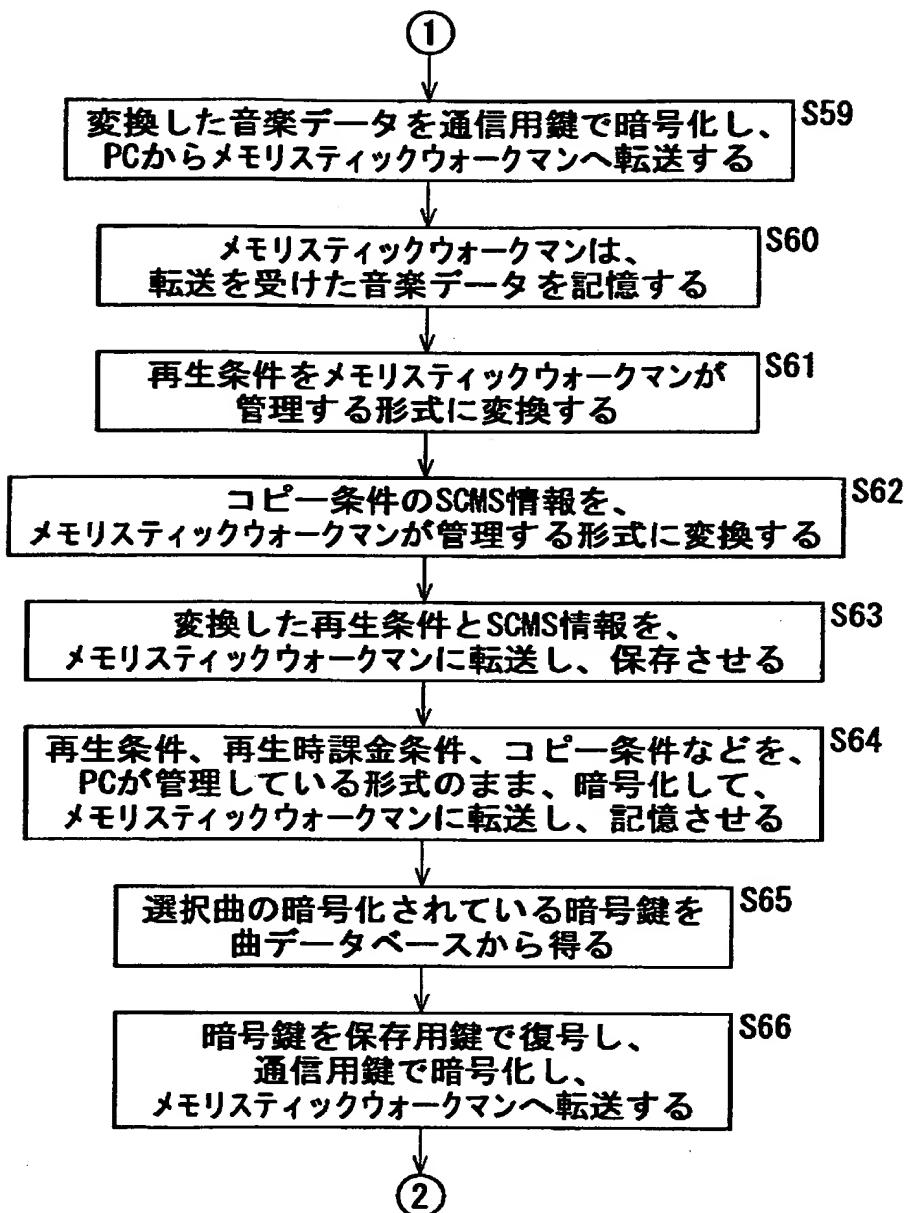
	アイテム1	アイテム2	アイテム3
ファイル名	xd000110.at2	px92341234.at2	aa0234287034.at2
暗号化された暗号鍵	0xabababababab	0x9898989898989899	0x123456789012
曲名	春の川	運命	荒城の月
長さ	180	190	200
再生条件:開始日時	-	2001.01.01.00:00	-
再生条件:終了日時	1999.07.31.23:59	-	-
再生条件:回数制限	-	20	-
再生回数力вшт	-	12	-
再生時課金条件	-	-	¥5
コピー条件:回数	2	0	0
コピー回数カウンタ	1	0	0
コピー条件:SCMS	0b01	0b10	0b00

ハッシュ値	0xf9951e566321
-------	----------------

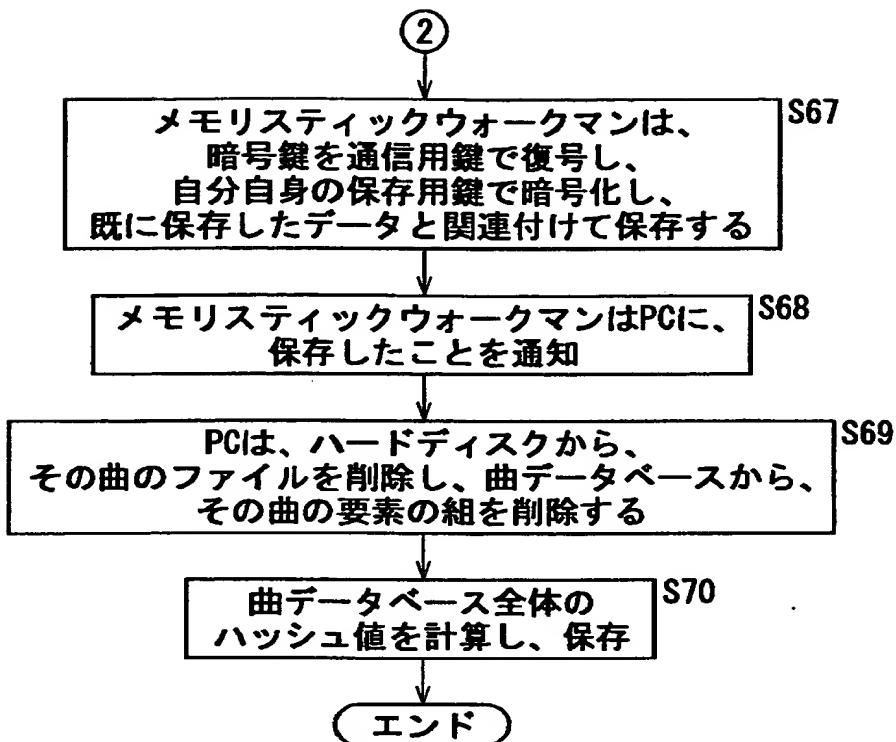
【図7】



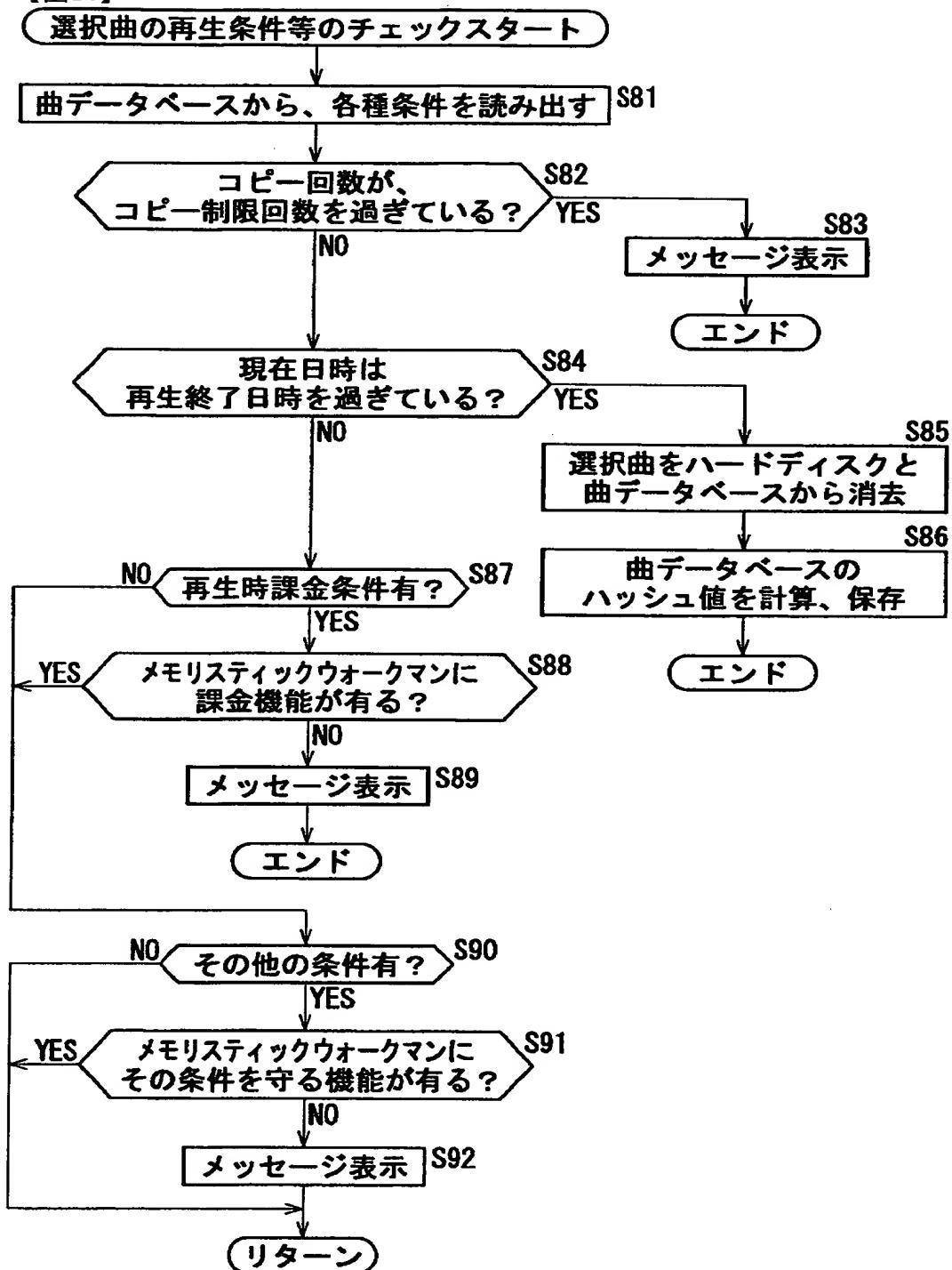
【図8】



【図9】



【図10】

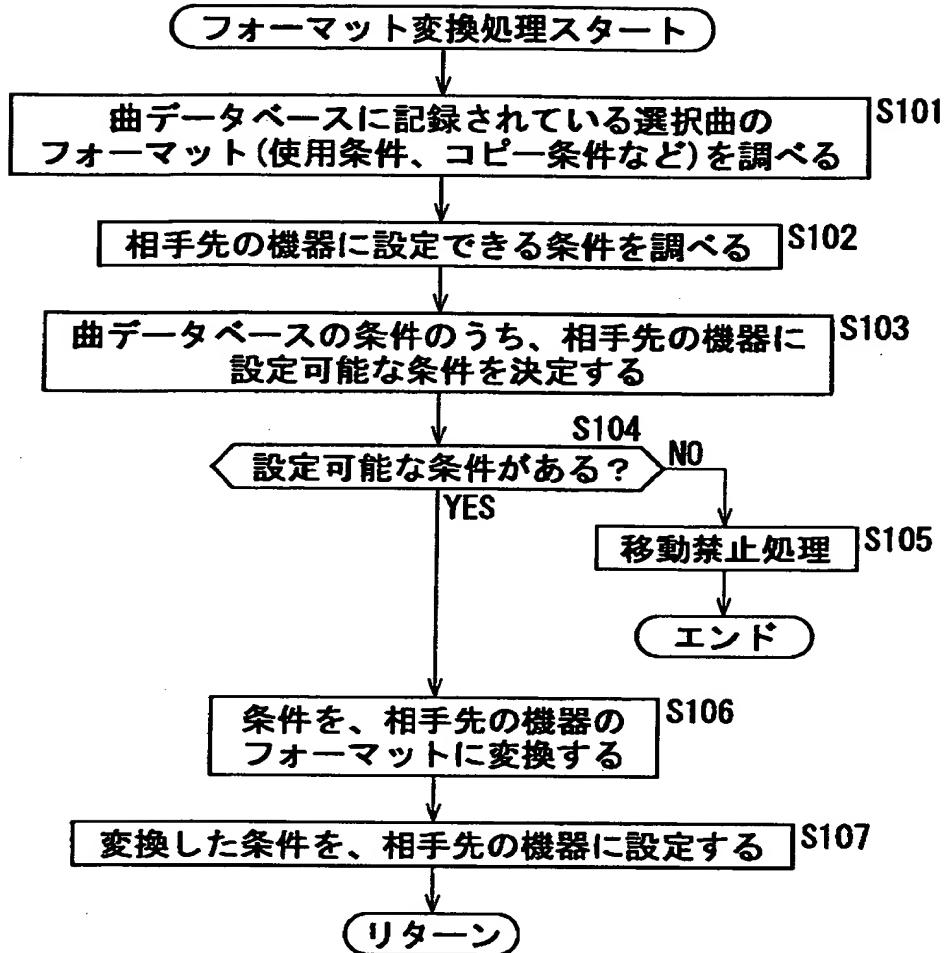


【図11】

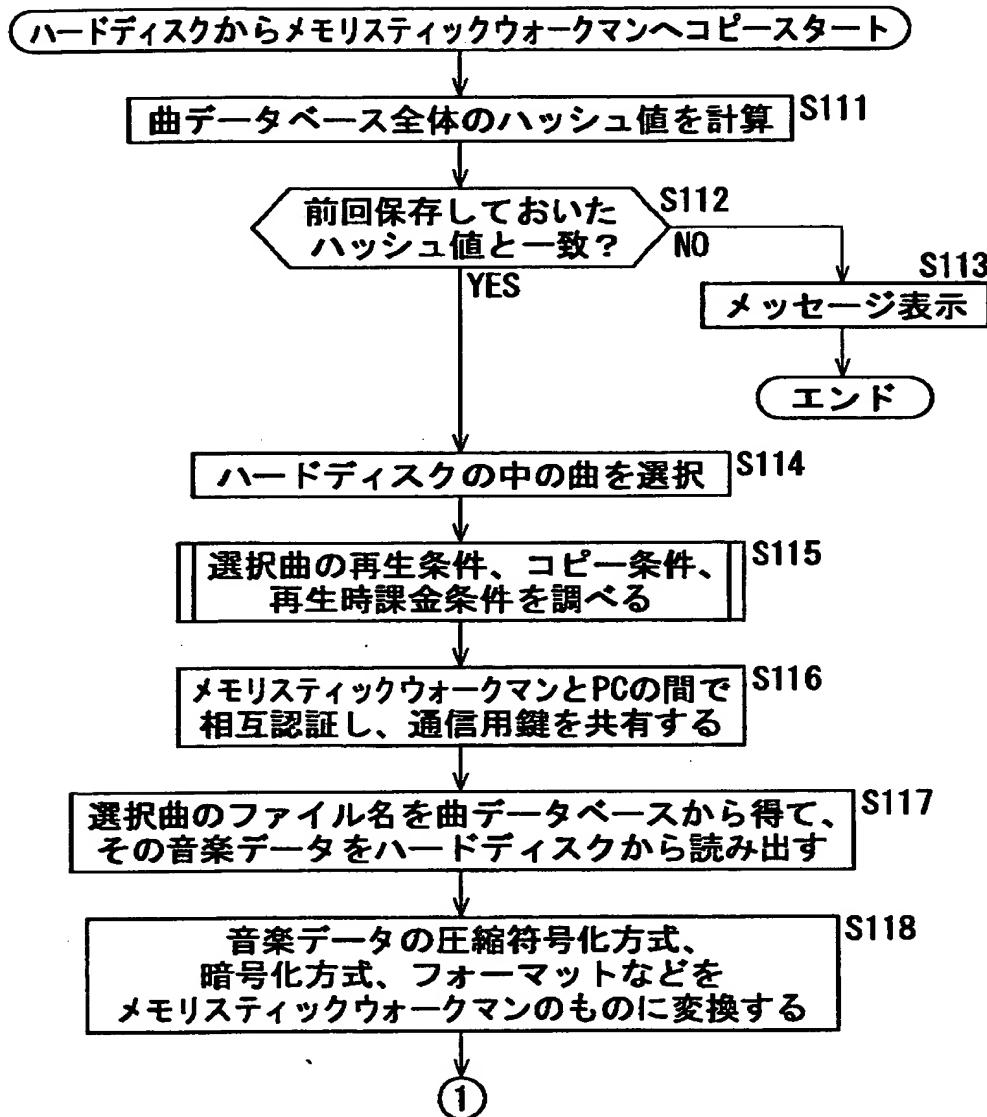
メモリスティックウォークマンが管理している再生条件

曲ID	アイテム1	アイテム2	アイテム3
	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

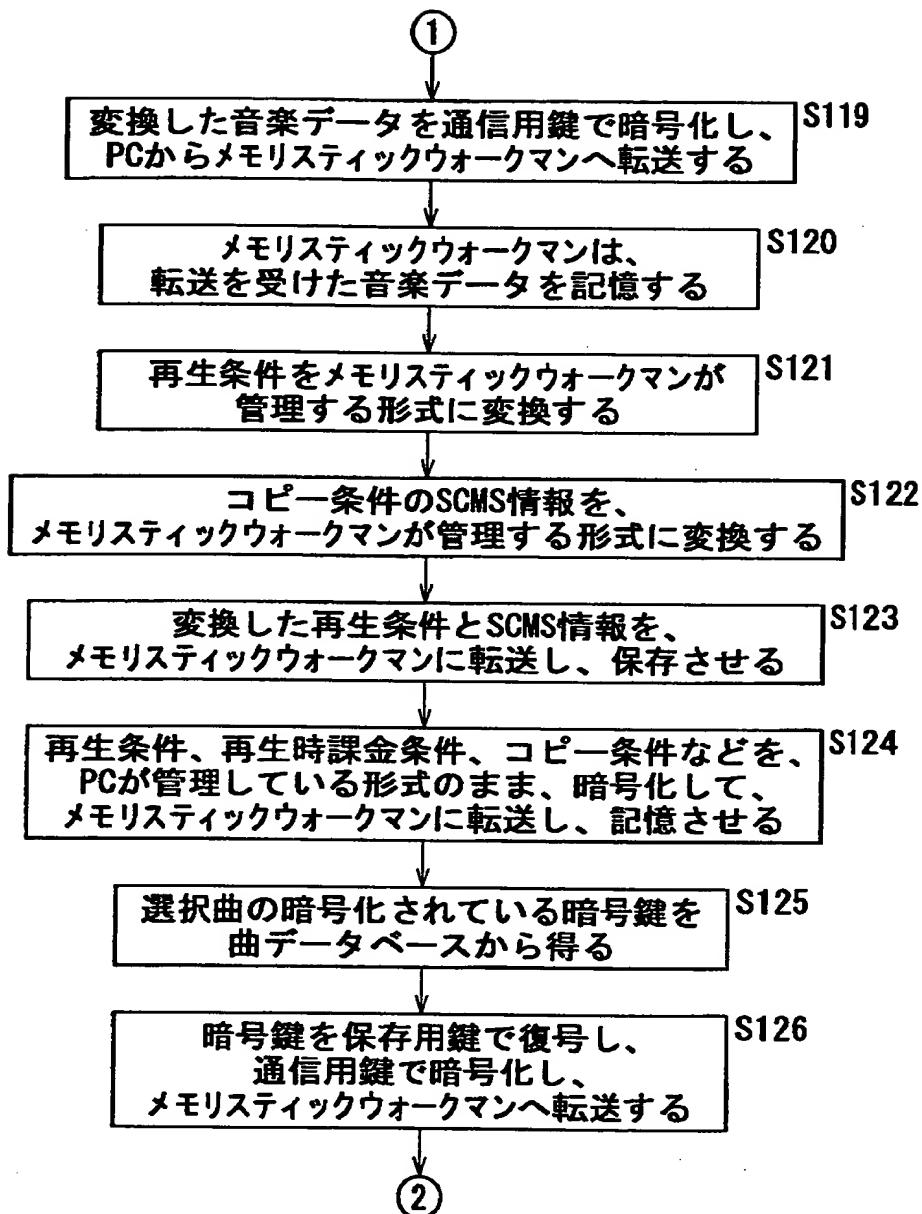
【図12】



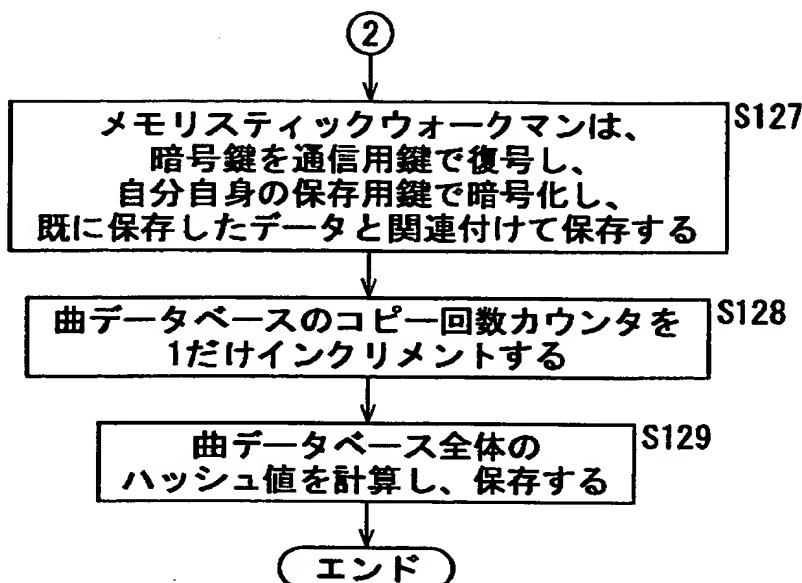
【図13】



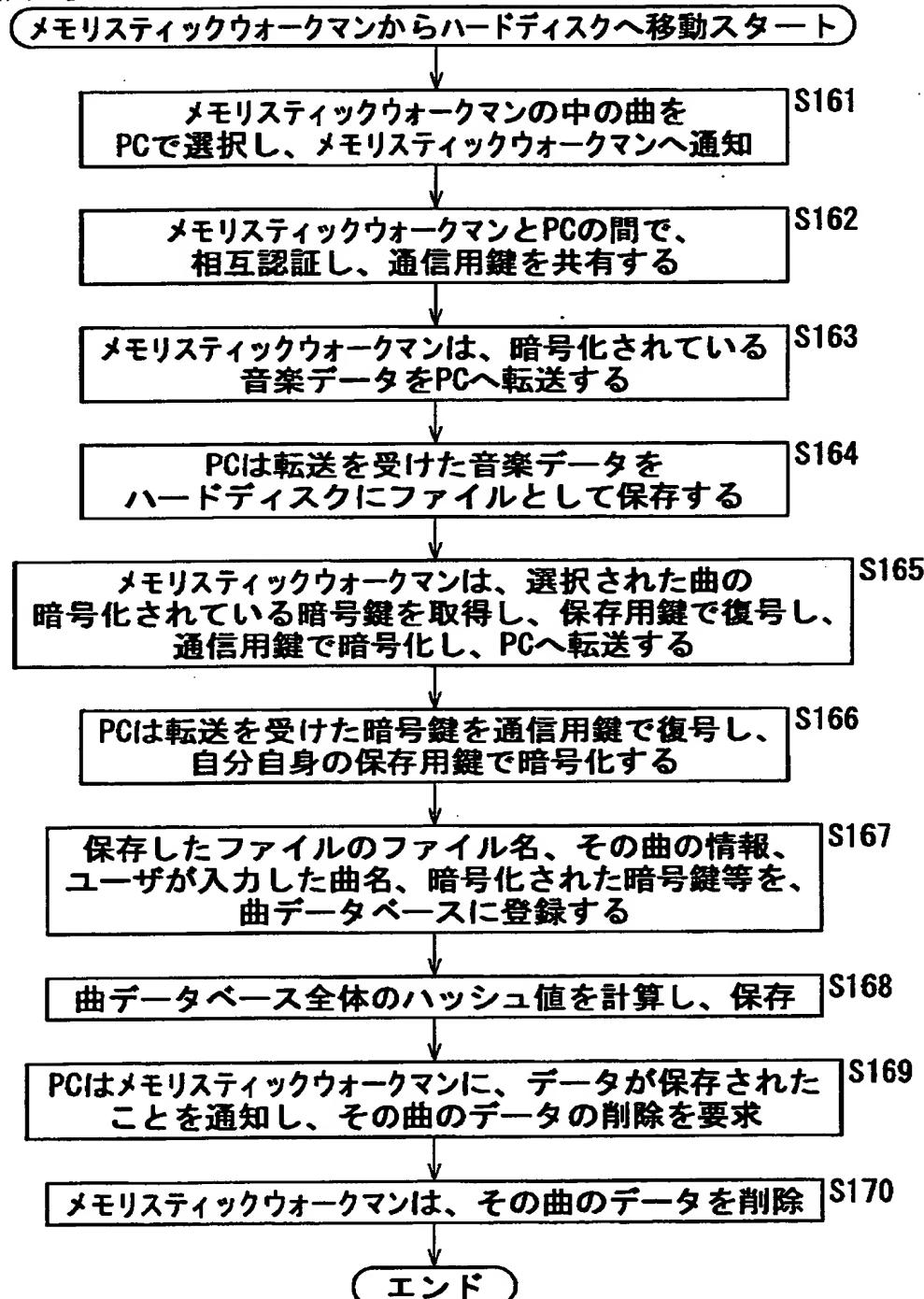
【図14】



【図15】



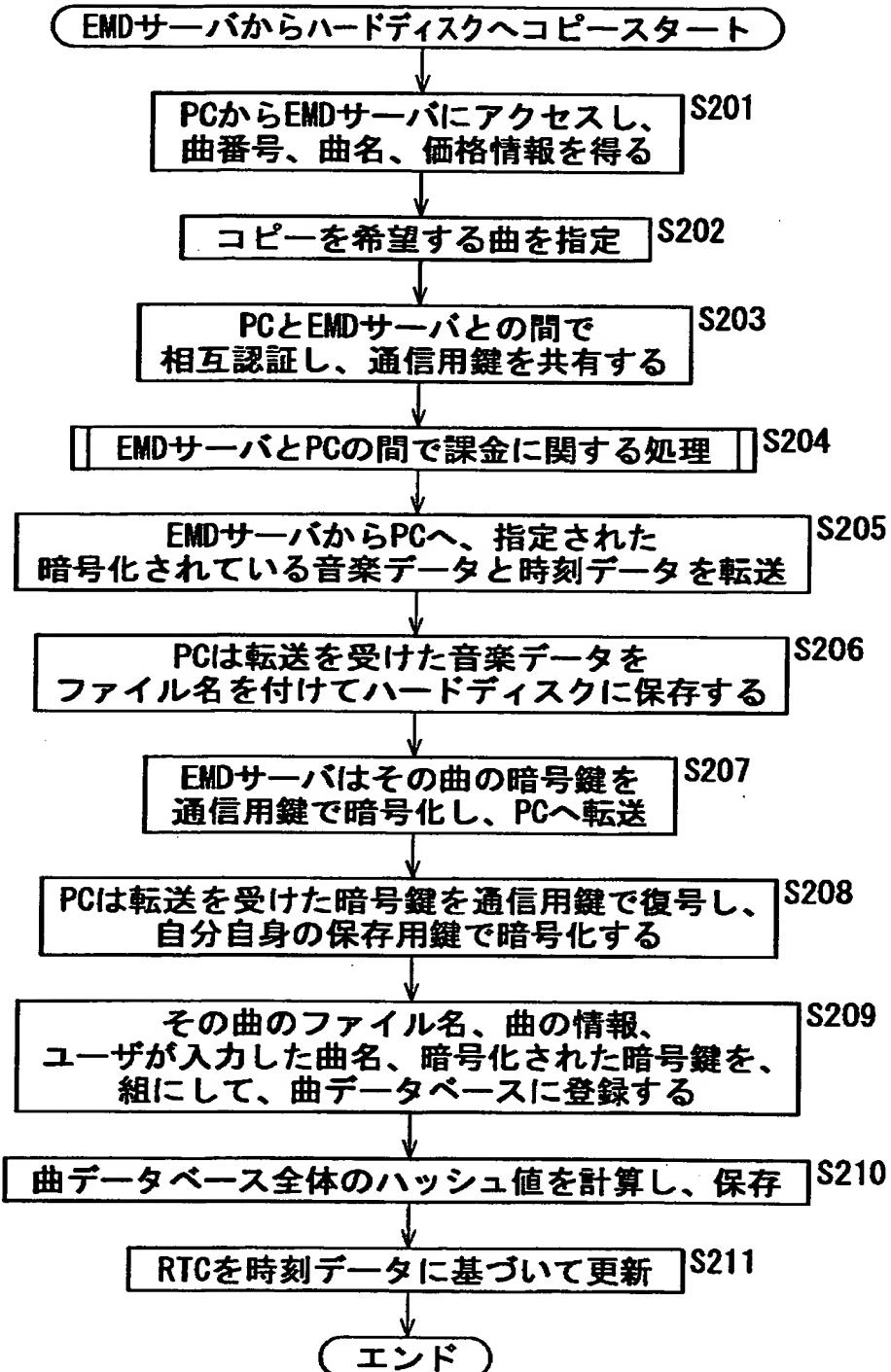
【図16】



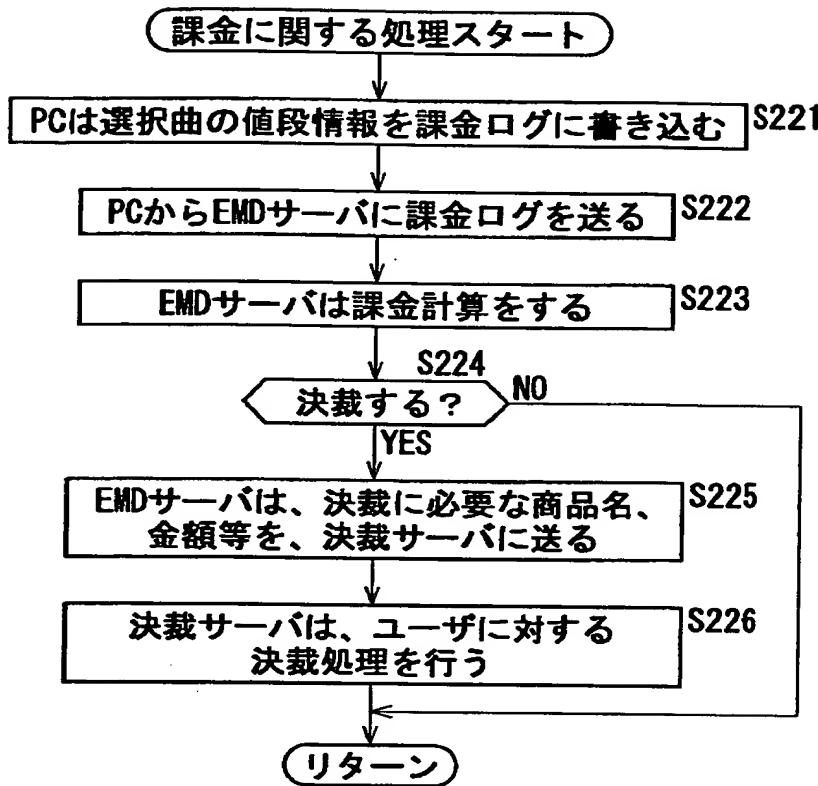
【図17】



【図18】



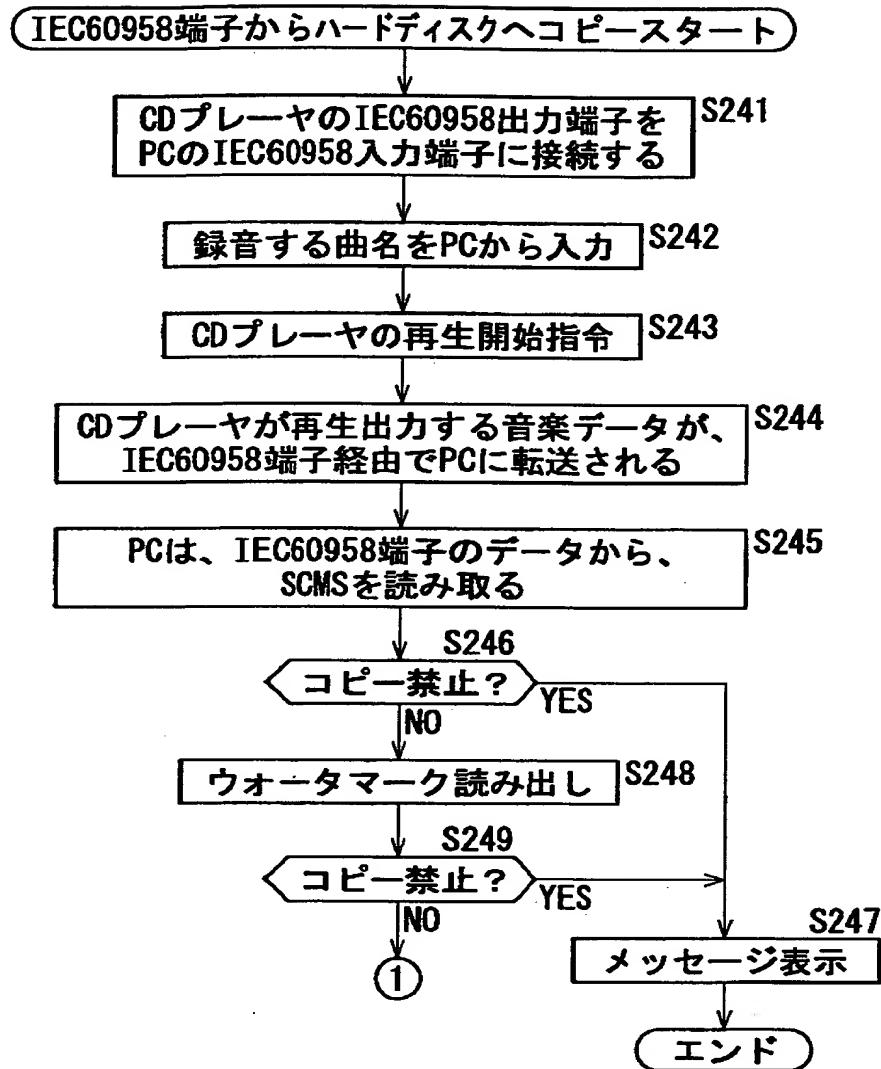
【図19】



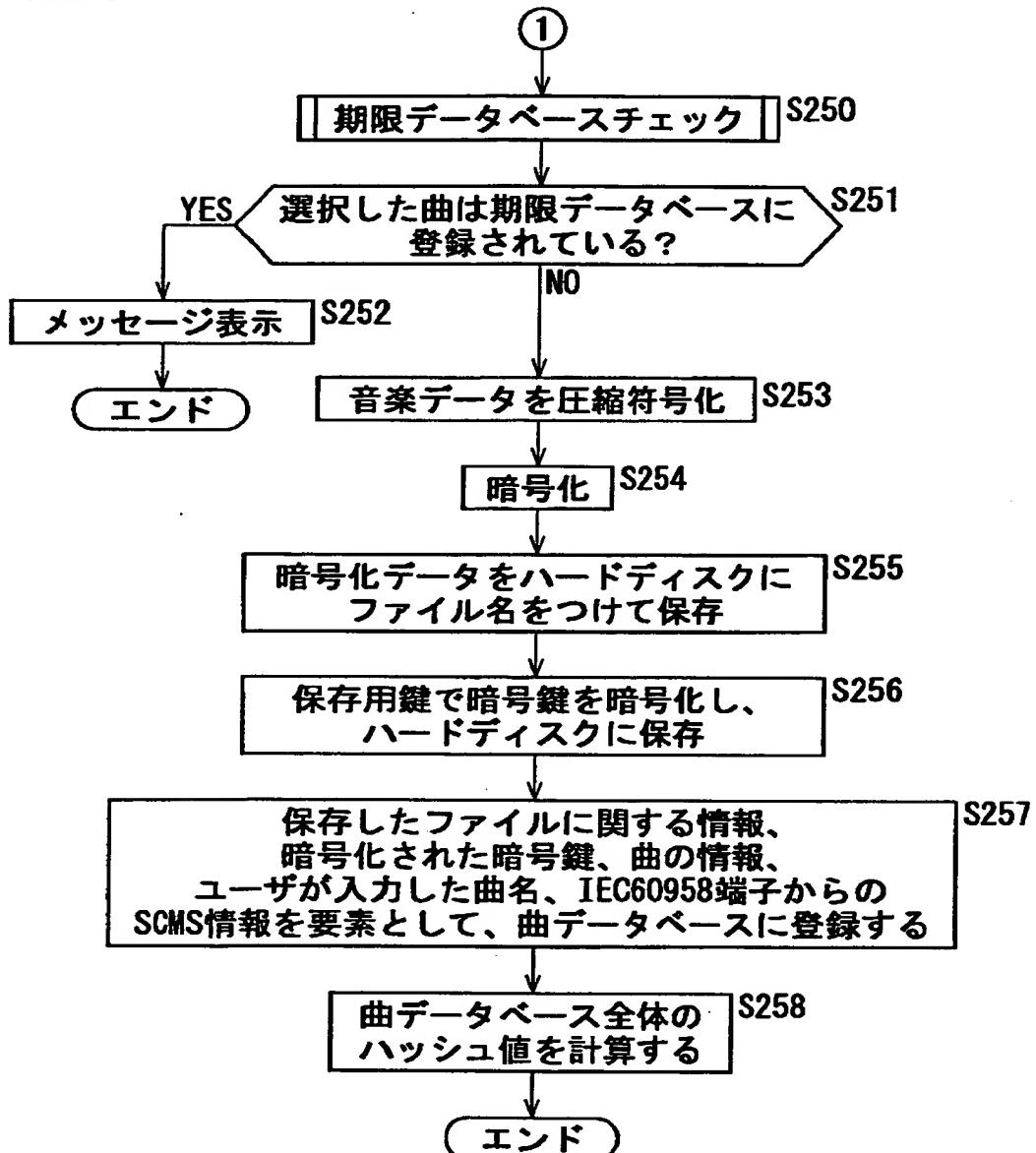
【図20】

課金ログ			
	アイテム1	アイテム2	アイテム3
料金	50	50	60
ハッシュ値	0xf8783e263517		

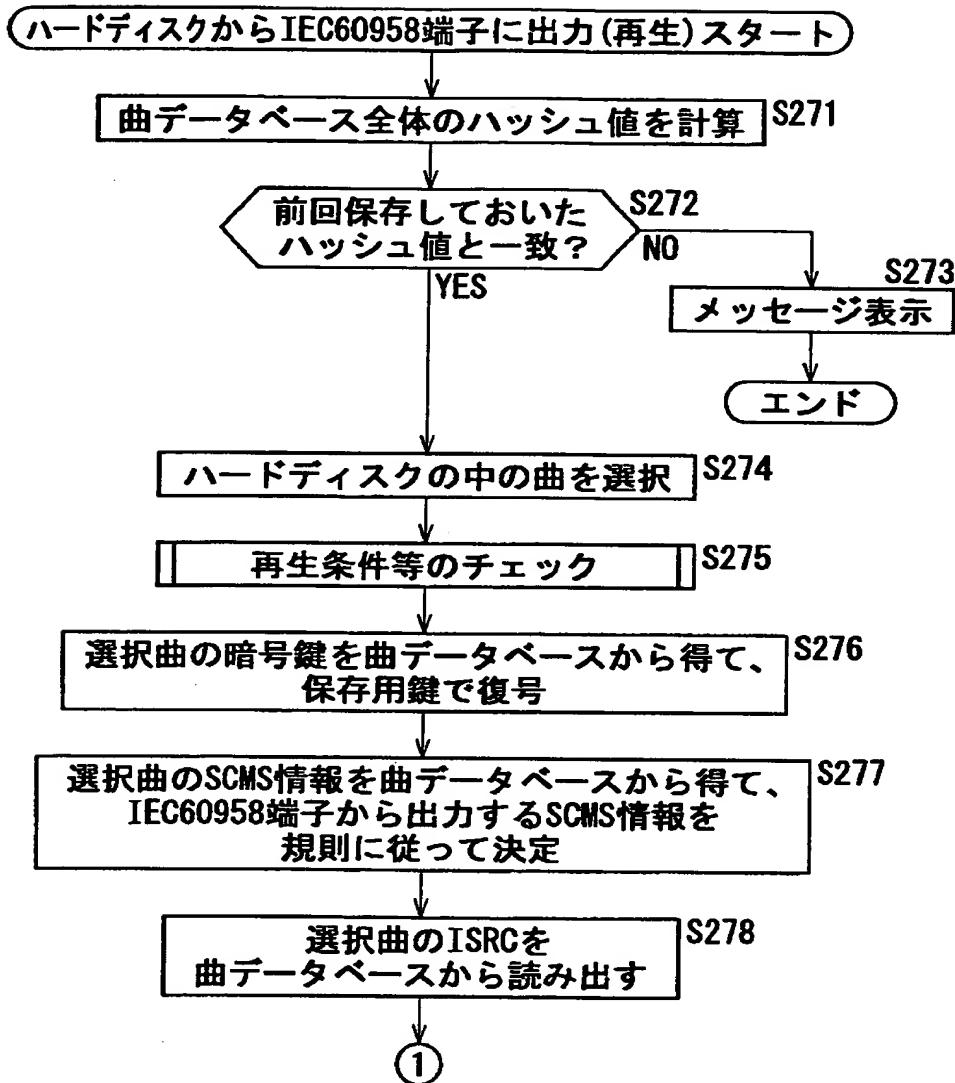
【図21】



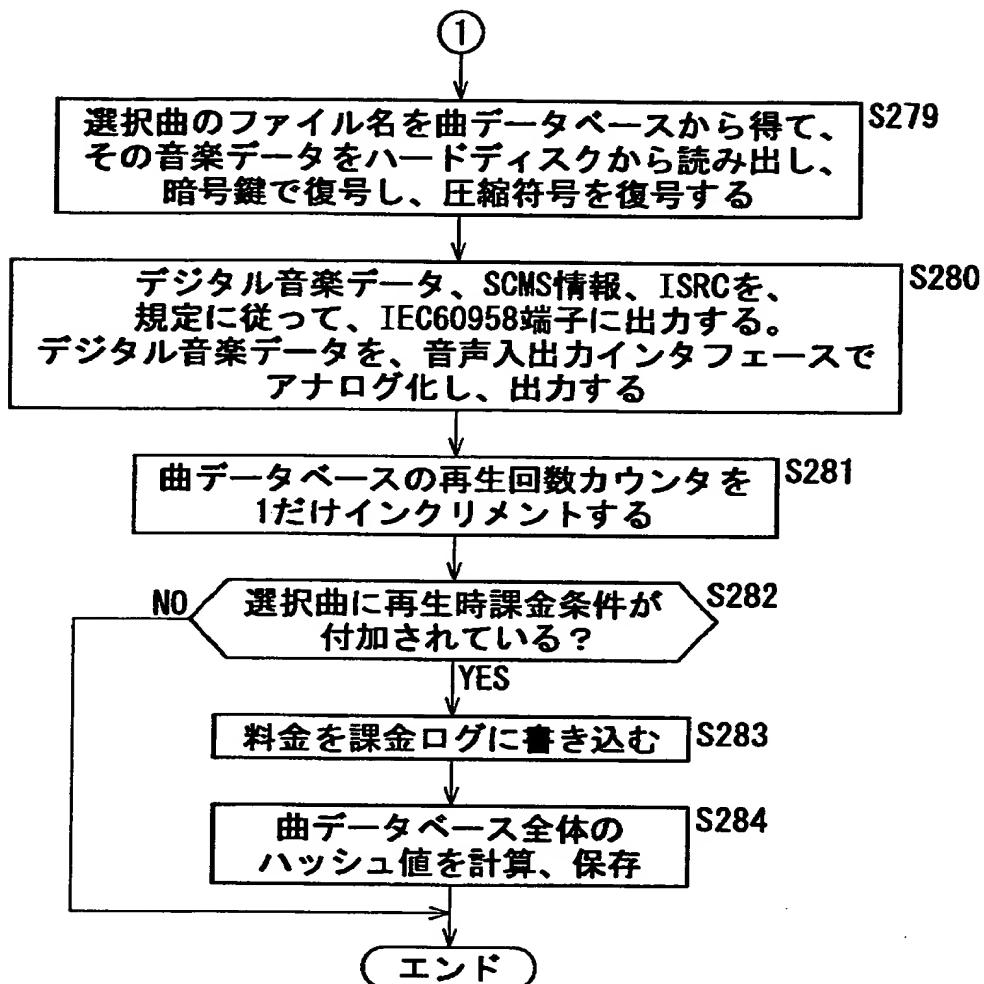
【図22】



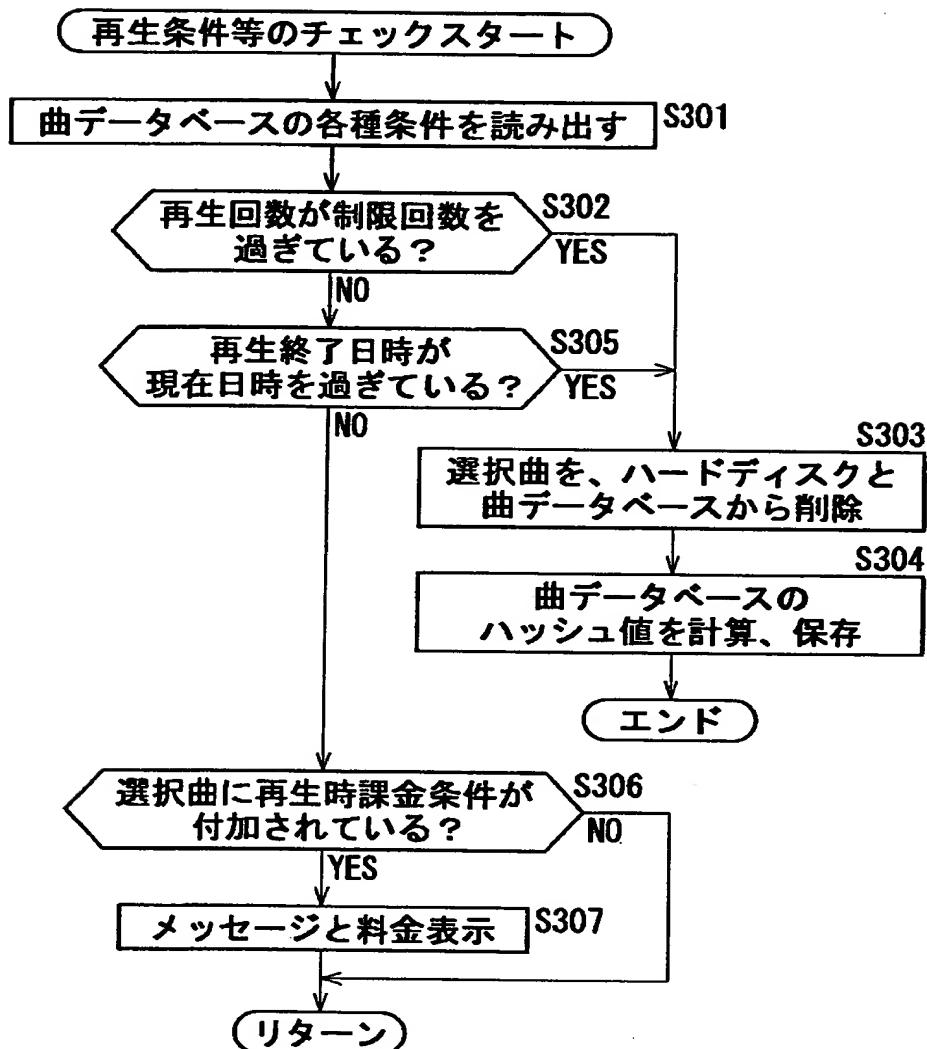
【図23】



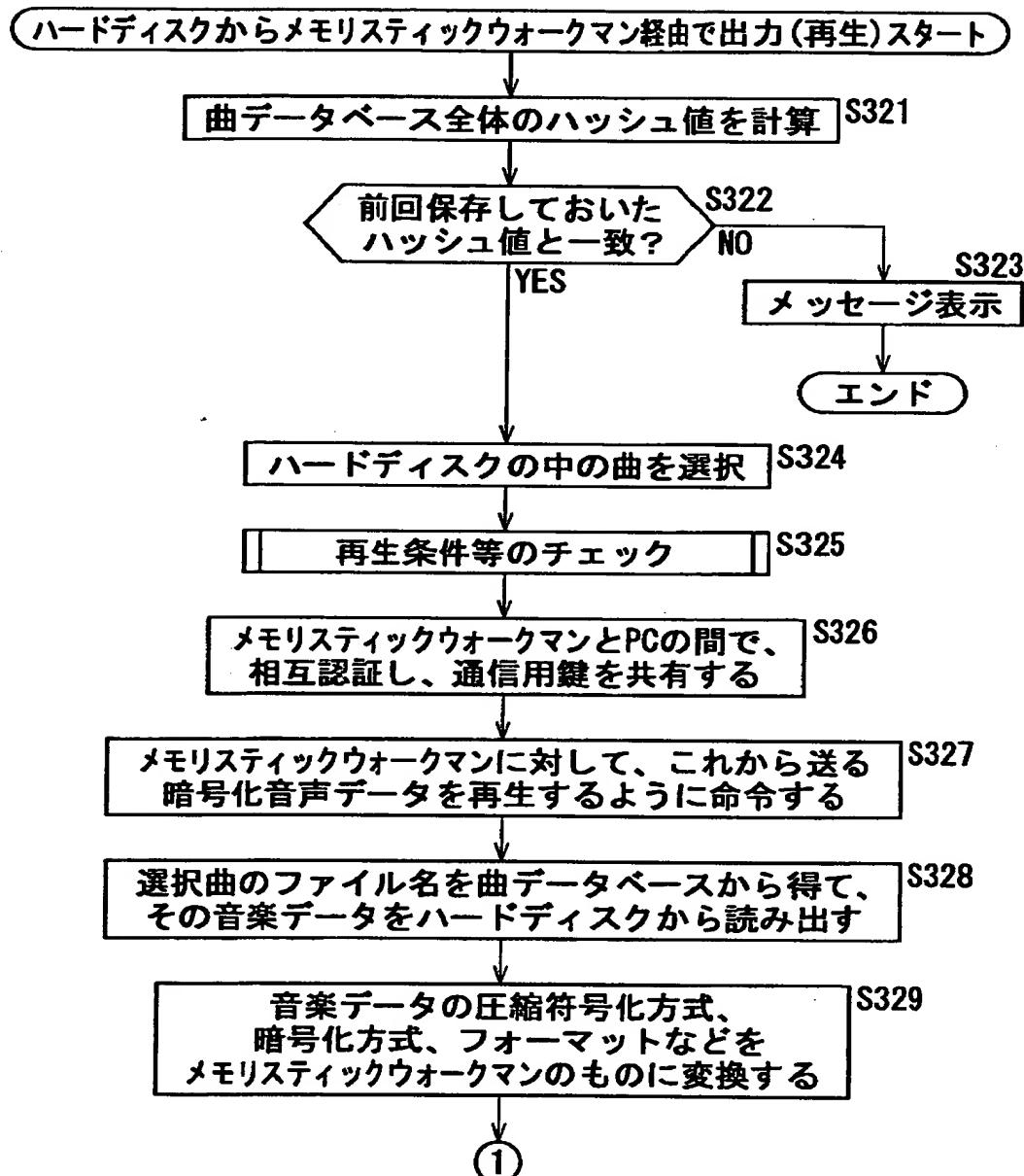
【図24】



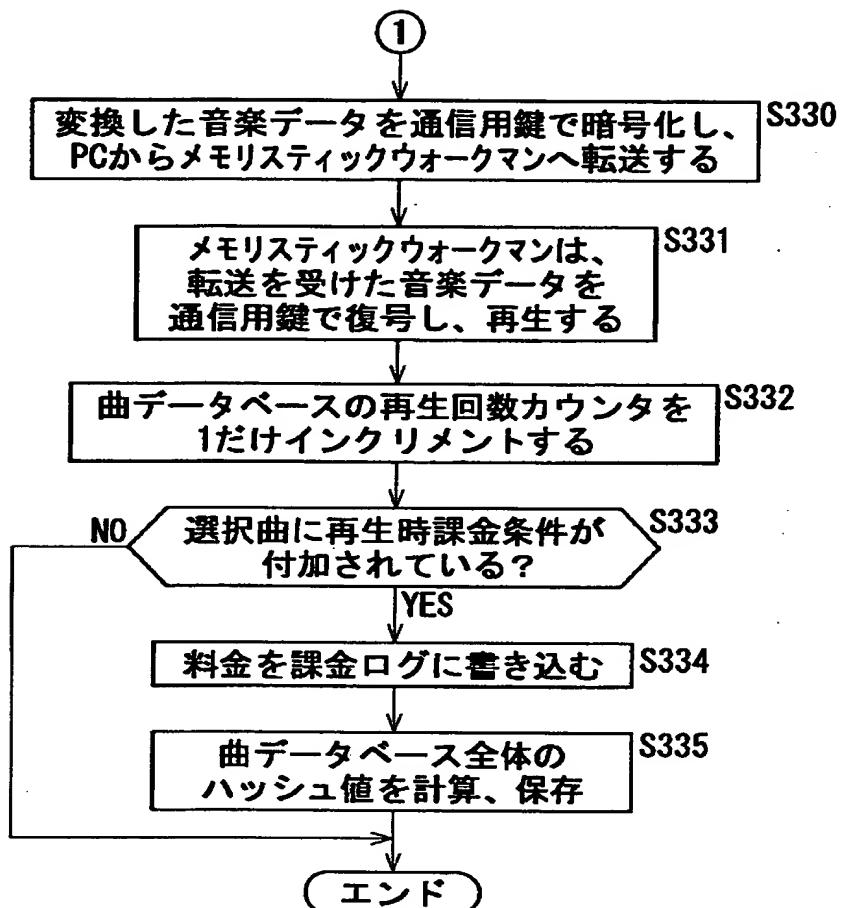
【図25】



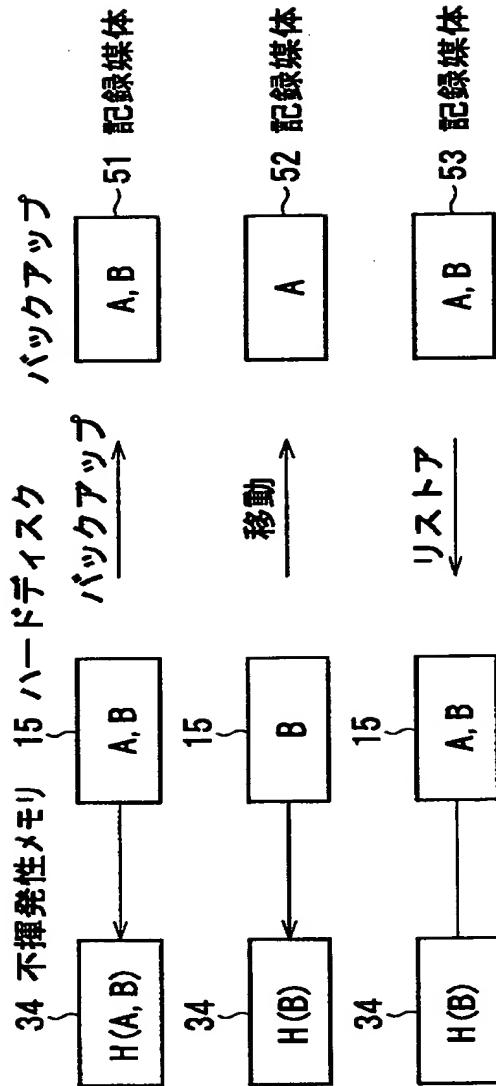
【図26】



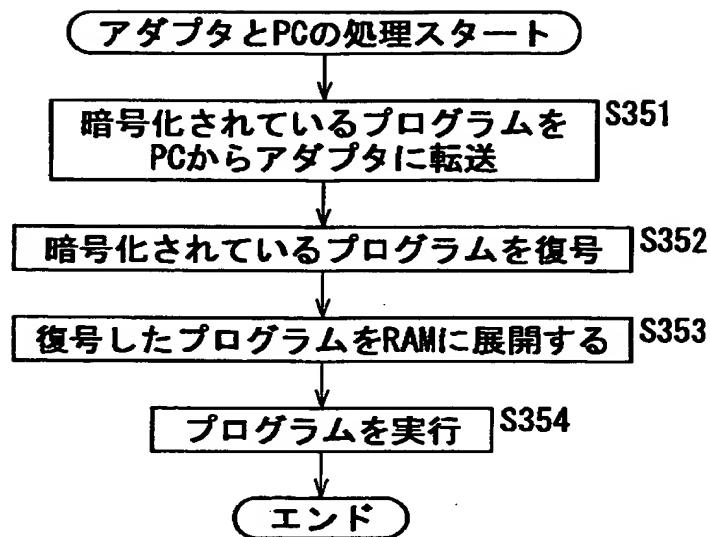
【図27】



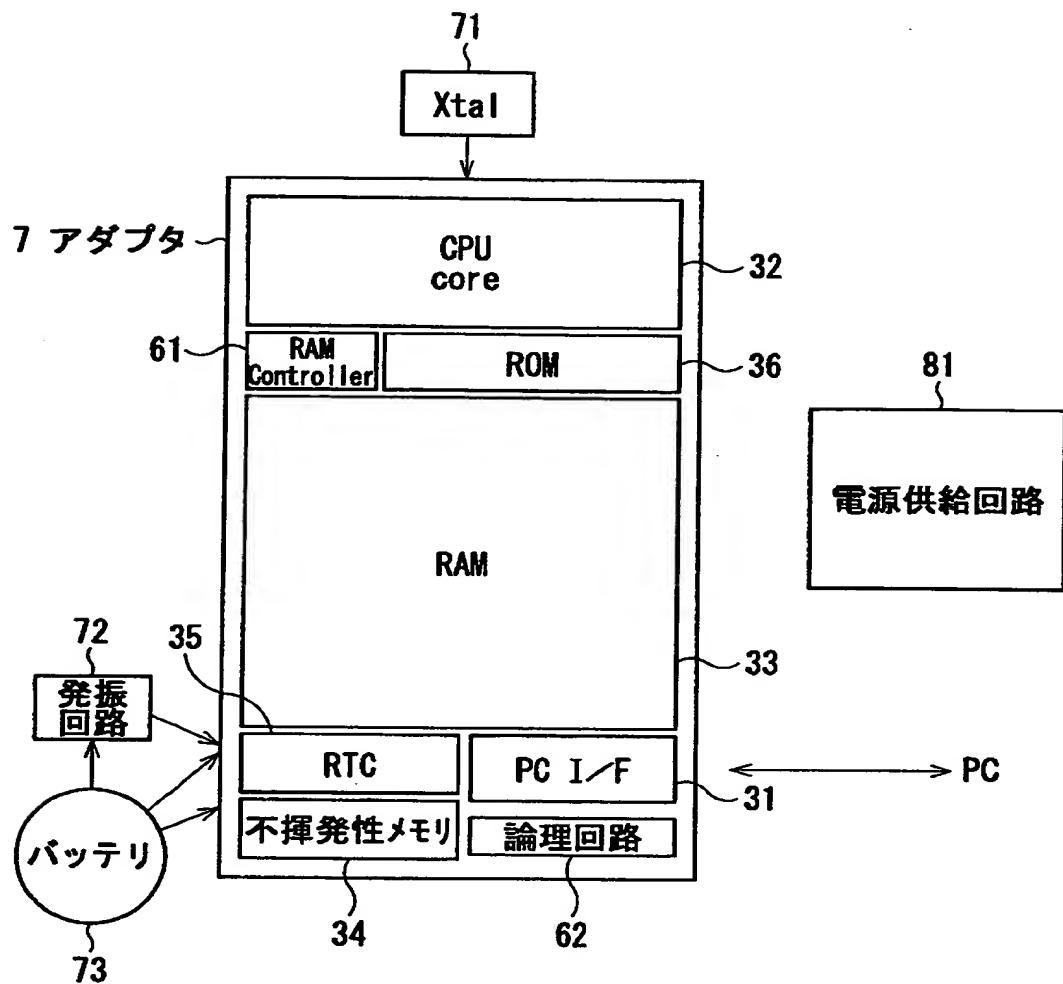
【図28】



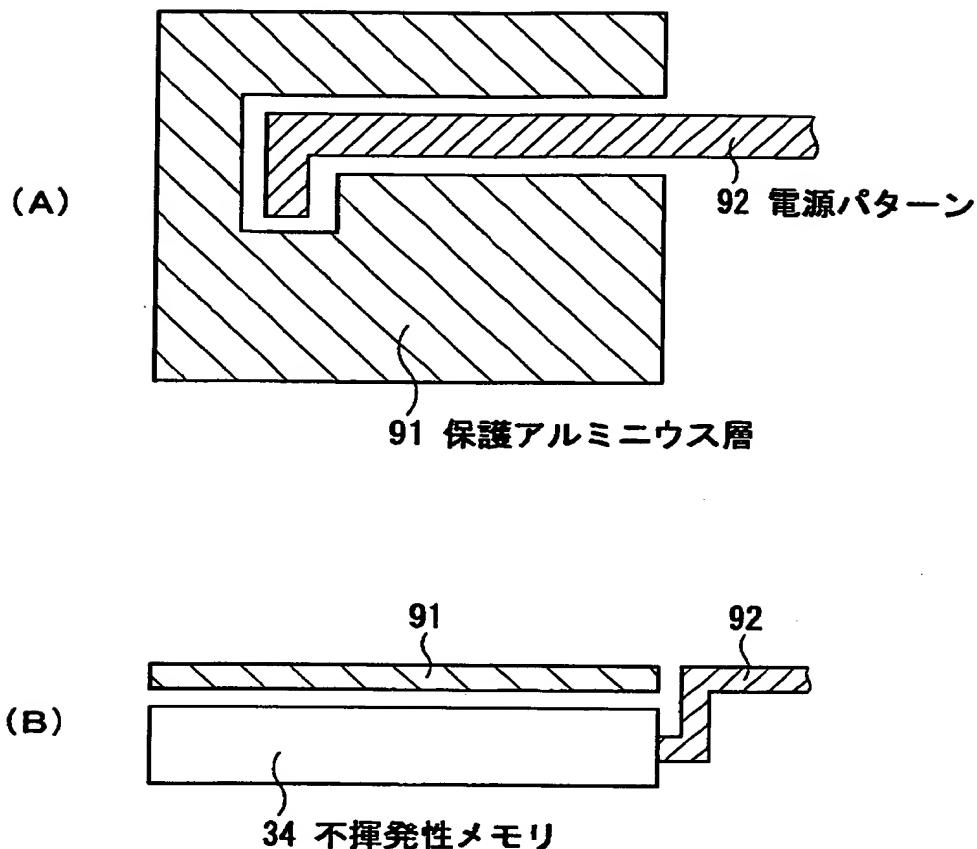
【図29】



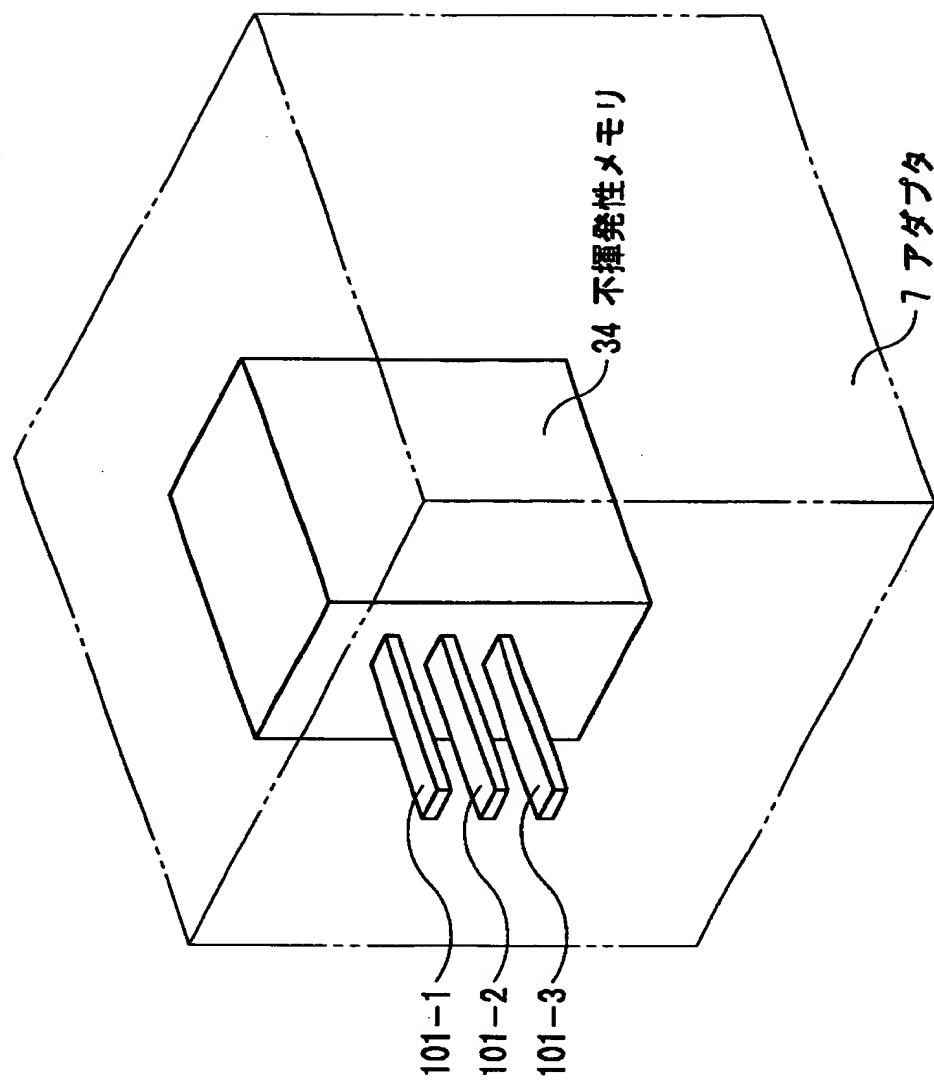
【図30】



【図31】



【図32】



【書類名】 要約書

【要約】

【課題】 ソフトウェアを解析し、改竄して、著作物を不正に複製することを防止する。

【解決手段】 パーソナルコンピュータ1のCPU12は、ハードディスク15に記録されている音楽データを管理する曲データベースのハッシュ値を、半導体ICよりなるアダプタ7のCPU32により演算させ、不揮発性メモリ34に記憶させる。ハードディスク15に記録されている音楽データを再生するとき、CPU12は、ハードディスク15の曲データベースのハッシュ値を計算し、不揮発性メモリ34に記憶されているそれまでのハッシュ値と比較し、その比較結果に対応して、ハードディスク15からの音楽データの再生を制御する。

【選択図】 図1

出願人履歴情報

識別番号 [00002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社